2011 Cost of Cyber Crime

West Virginia Cyber Security Event

Sponsored by HP

Independently conducted by Ponemon Institute

5 October 2011

Ponemon Institute LLC

- ✓ The Institute is dedicated to advancing responsible information management practices that positively affect privacy and data protection in business and government.
- ✓ The Institute conducts independent research, educates leaders from the private and public sectors and verifies the privacy and data protection practices of organizations.
- ✓ Ponemon Institute is a full member of **CASRO** (Council of American Survey Research Organizations). Dr. Ponemon serves as CASRO's chairman of Government & Public Affairs Committee of the Board.
- ✓ The Institute has assembled more than 60 leading multinational corporations called the **RIM Council**, which focuses the development and execution of ethical principles for the collection and use of personal data about people and households.
- ✓ The majority of active participants are privacy or information security leaders.

Summary of key findings

- **Cyber crimes continue to be very costly for organizations**. We found that the average annualized cost for 50 benchmarked organizations is $8.4 million per year, with a range from $1.5 million to $36.5 million. Last year's average cost per benchmarked organization was $6.5 million. Thus, we observe a $1.9 million (26 percent) cost increase.
- **Cyber crime cost varies by organizational size.** Results reveal a positive relationship between organizational size (as measured by enterprise seats) and annualized cost. However, relative to each enterprise seat, smaller organizations incur a much higher per capita cost than larger organizations ($1,088 versus $284).
- **Cyber crimes are intrusive and common occurrences**. The companies participating in our study experienced 72 successful attacks per week – or more than 1.4 successful attacks per organization each week. Last year's study reported 50 successful attacks on average per week.
- **The most costly cyber crimes are those caused by malicious code, denial of service, stolen or hijacked devices and malicious insiders.** These account for more than 90 percent of all cyber crime costs per organization on an annual basis. Mitigation of such attacks requires enabling technologies such as SIEM and enterprise GRC solutions.
- **Cyber attacks can get costly if not resolved quickly.** Results show a positive relationship between the time to contain an attack and organizational cost. The average time to resolve a cyber attack is 18 days, with an average cost to participating organizations of $415,748 over this 18 day period. This represents a 67 percent increase from last year's estimated average cost of $247,744, which is compiled for a 14 day period. Results show that malicious insider attacks can take more than 45 days on average to contain. .

Summary of key findings

- **Information theft continues to represent the highest external cost, followed by the costs associated with business disruption.** On an annualized basis, information theft accounts for 40 percent of total external costs (down 2 percent from 2010). Costs associated with disruption to business or lost productivity accounts for 28 percent of external costs (up 6 percent from 2010).
- **Recovery and detection are the most costly internal activities**. On an annualized basis, recovery and detection combined account for 45 percent of the total internal activity cost with cash outlays and labor representing the majority of these costs.
- **All industries fall victim to cybercrime.** The average annualized cost of cyber crime appears to vary by industry segment, where defense, utilities & energy, and financial service companies experience higher costs than organizations in retail, hospitality and consumer products.
- **A strong security posture moderates the cost of cyber attacks**. We utilize a well-known metric called the Security Effectiveness Score (SES) to define an organization's ability to achieve reasonable security objectives. The higher the SES, the more effective the organization is in achieving its security objectives. The average cost to mitigate a cyber attack for organizations with a high SES is substantially lower than organizations with a low SES score.
- **Enterprise deployment of GRC and SIEM makes a difference**. The cost of cyber crime is moderated by GRC practices. Similarly, companies that had deployed a SIEM system achieved cost savings when dealing with cyber attacks in comparison to those organizations that had not.

Benchmark Methods & Background

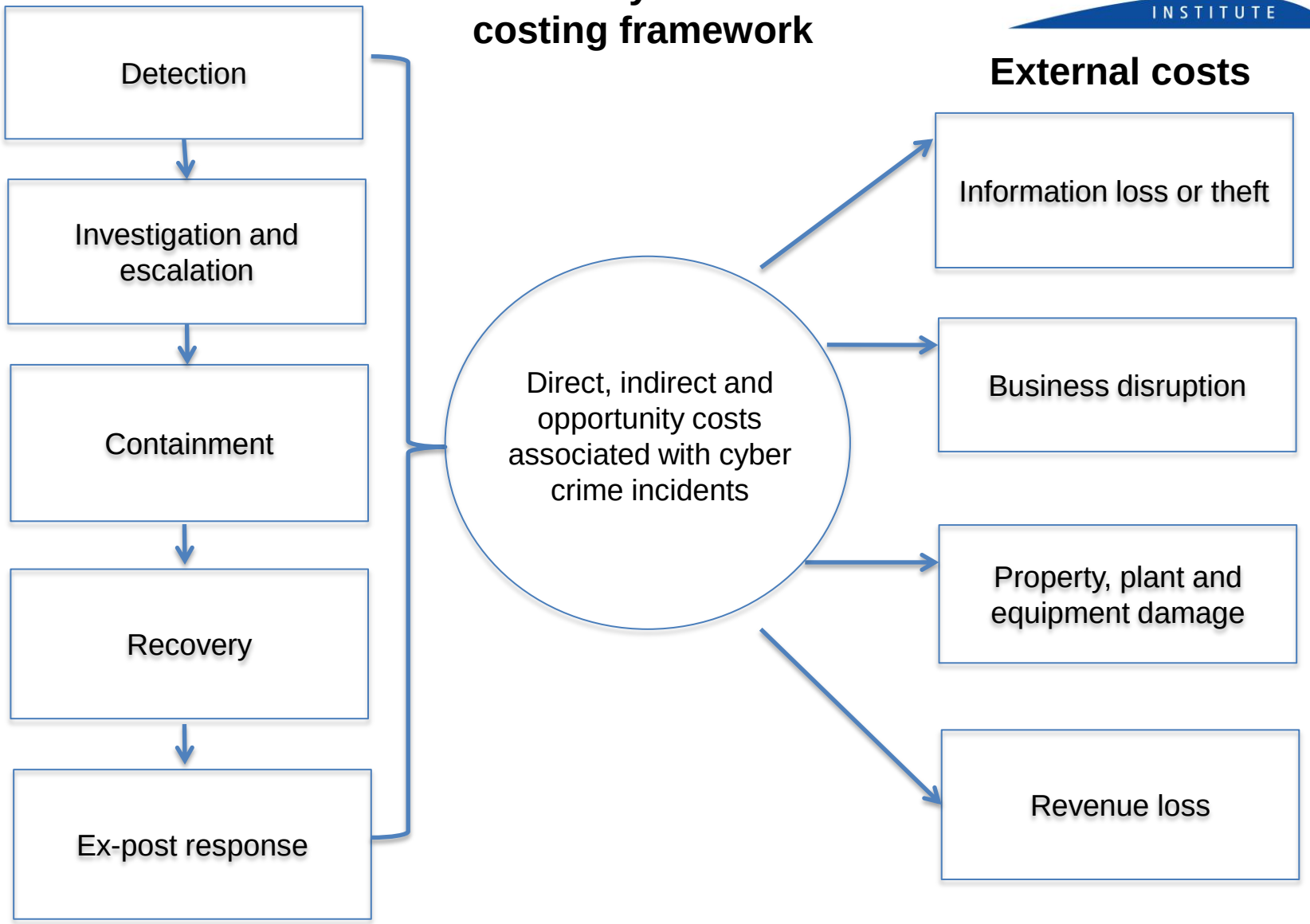
About our study

- We conducted the second annual study that attempts to rigorously measure the cost of cyber crime experienced by a representative sample of U.S. organizations matched for purposes of comparison to our 2010 study.
- We contacted nearly 400 organizations for possible participation in our study.
- Initially, 63 organizations agreed to participate.
- 50 organizations completed the full analysis and met our size criteria (minimum enterprise seats at 700). This is an increase of 5 organizations from FY 2010.
- Our methods involved benchmarks and activity-based costing (ABC) over a four-week period for each case study.
- Cost estimates were captured using a standardized instrument for both direct and indirect cost categories.
- Labor (productivity) and overhead costs were allocated to five internal activity centers (see framework slide).
- External costs include the loss of information assets, business disruption, revenue loss, and equipment damages.
- Extrapolated costs for nine discernible attack vectors were analyzed.

Internal costs

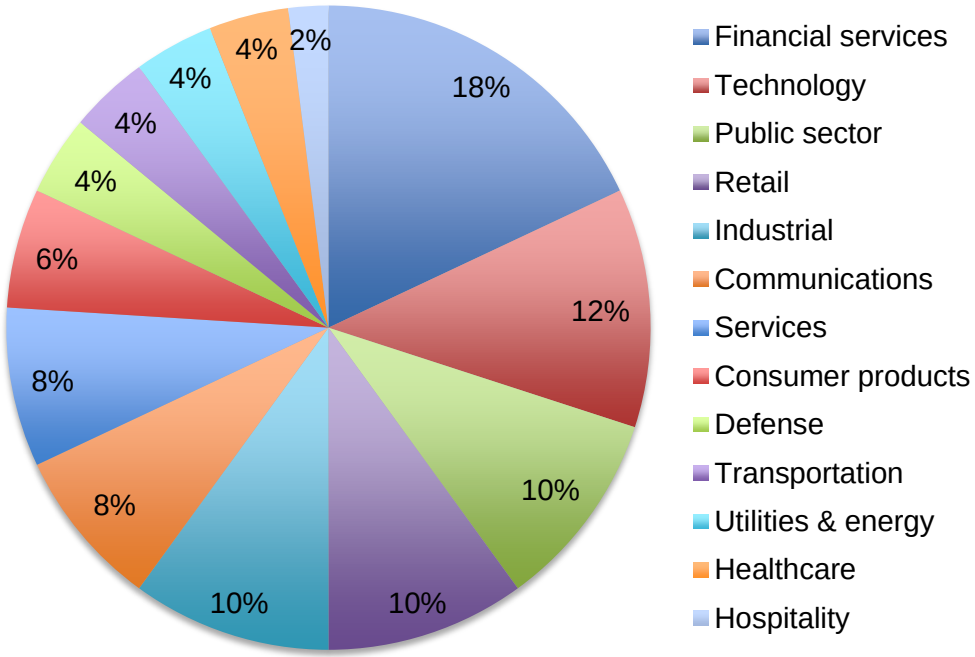
Activity-based costing framework

External costs



About industries

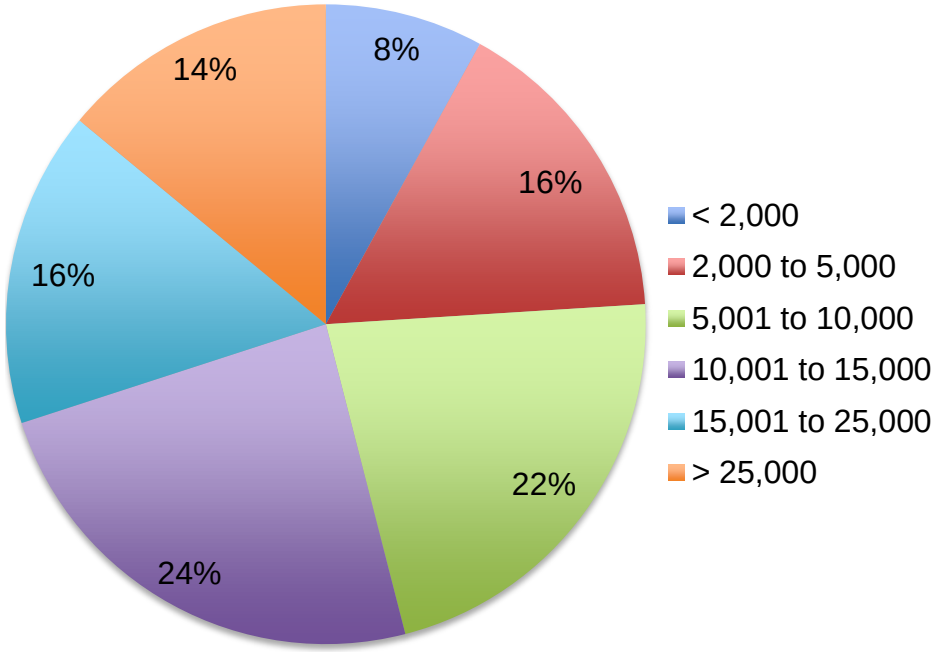
Our sample consists of 50 organizations located in the United States with a set minimum of 500 seats. The range of enterprise seats is 700 to over 139,000. All research was conducted over a six-month period concluding on June 17, 2011. The final benchmark sample contained 13 industry sectors.



Industry	FY 2011	FY 2010
Financial services	9	10
Technology	6	5
Public sector	5	4
Retail	5	4
Industrial	5	4
Communications	4	5
Services	4	3
Consumer products	3	4
Defense	2	1
Transportation	2	3
Utilities & energy	2	1
Healthcare	2	0
Hospitality	1	0
Education	0	1
Total	50	45

About enterprise seats (size)

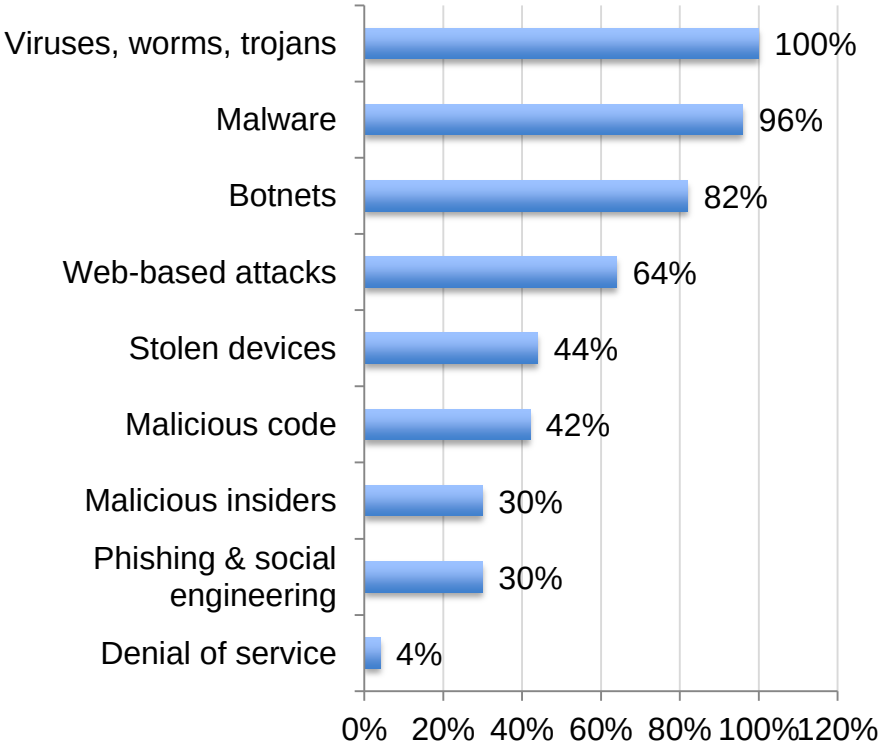
Our sample consists of 50 organizations located in the United States with a set minimum of 500 seats. The range of enterprise seats is 700 to over 139,000. All research was conducted over a six-month period concluding on June 17, 2011. The final benchmark sample contained 13 industry sectors.



Enterprise seats	FY 2011	FY 2010
< 2,000	4	6
2,000 to 5,000	8	11
5,001 to 10,000	11	8
10,001 to 15,000	12	8
15,001 to 25,000	8	6
> 25,000	7	6
Total	50	45

Types of cyber attacks experienced

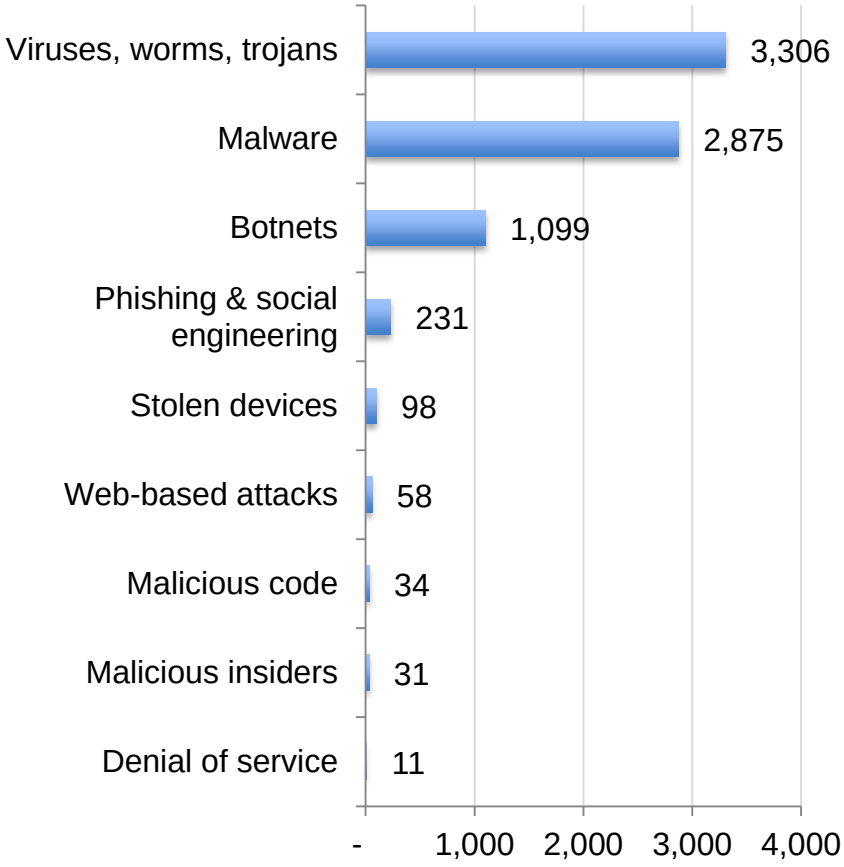
Our sample consists of 50 organizations located in the United States with a set minimum of 500 seats. The range of enterprise seats is 700 to over 139,000. All research was conducted over a six-month period concluding on June 17, 2011. The final benchmark sample contained 13 industry sectors.



Types of attacks	FY 2011	FY 2010
Viruses, worms, trojans	50	45
Malware	48	36
Botnets	41	33
Web-based attacks	32	24
Phishing & social engineering	15	17
Stolen devices	22	16
Malicious insiders	15	13
Malicious code	21	12
Denial of service	2	0

Frequency of cyber attacks experienced

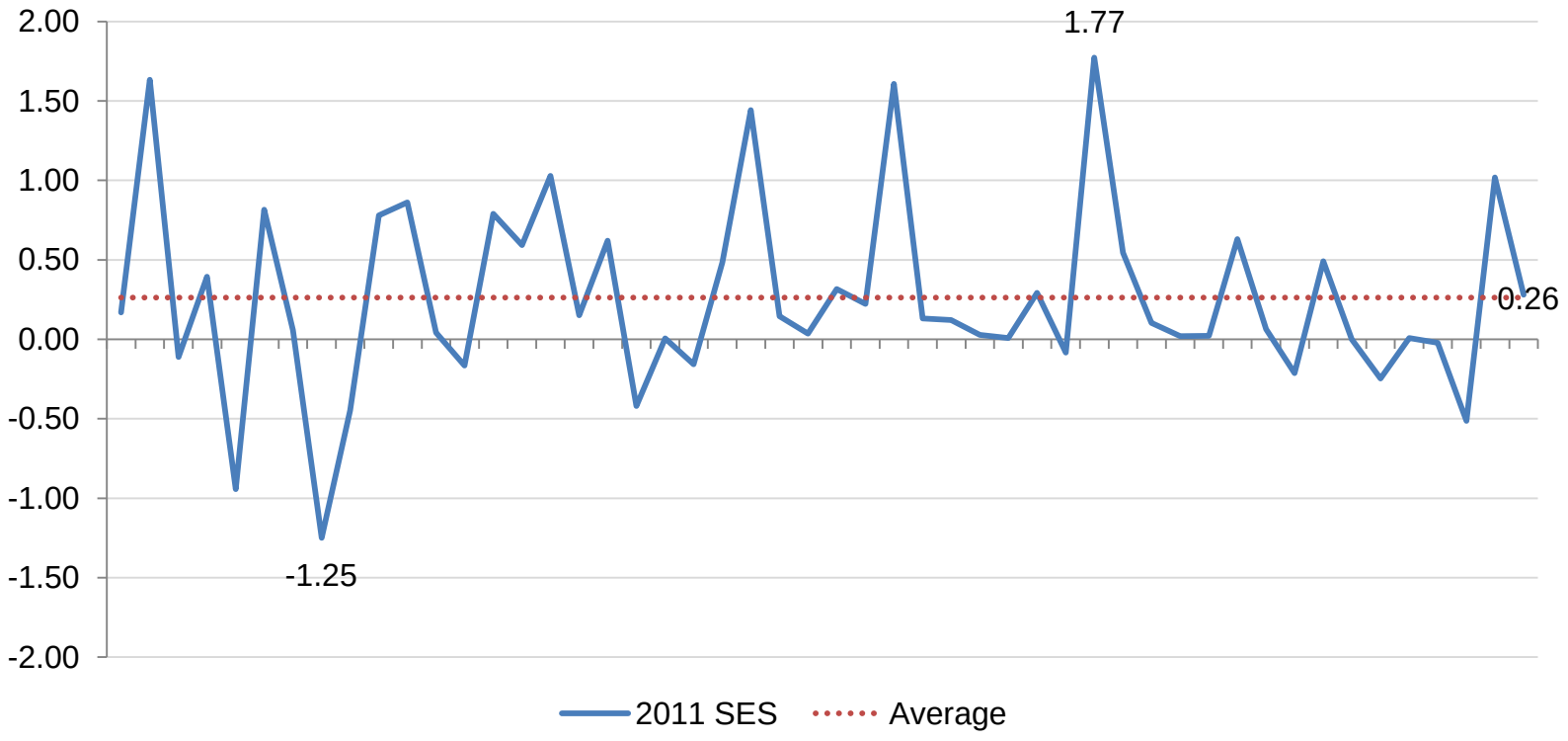
Our sample consists of 50 organizations located in the United States with a minimum of 500 seats. The range of enterprise seats is 700 to over 139,000. All research was conducted over a six-month period concluding on June 17, 2011. The final benchmark sample contained 13 industry sectors.



Frequency of attacks	FY 2011	FY 2010
Viruses, worms, trojans	3,306	2,215
Malware	2,875	1,243
Botnets	1,099	1,130
Phishing & social engineering	231	76
Stolen devices	98	64
Web-based attacks	58	27
Malicious code	49	29
Malicious insiders	31	27
Denial of service	11	-

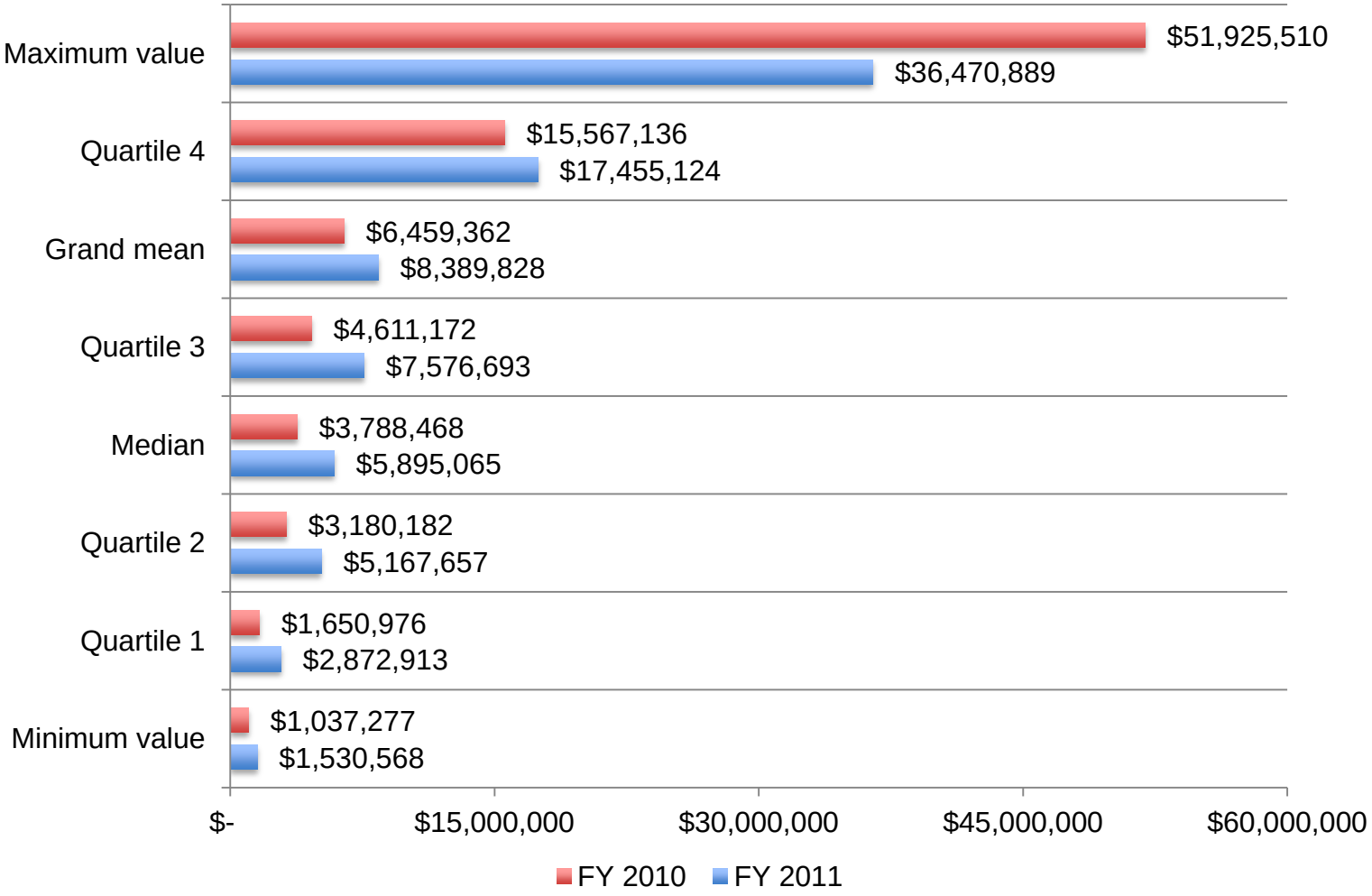
Security effectiveness score (SES) for 50 participating companies

The SES is a scoring method with a range of +2 to -2 (theoretical mean = 0). The FY 2011 benchmark sample provides a range of -1.25 (lowest SES) to+ 1.77 (highest SES) with a mean value of +.26. The mean SES for our 2010 benchmark sample was +.29.

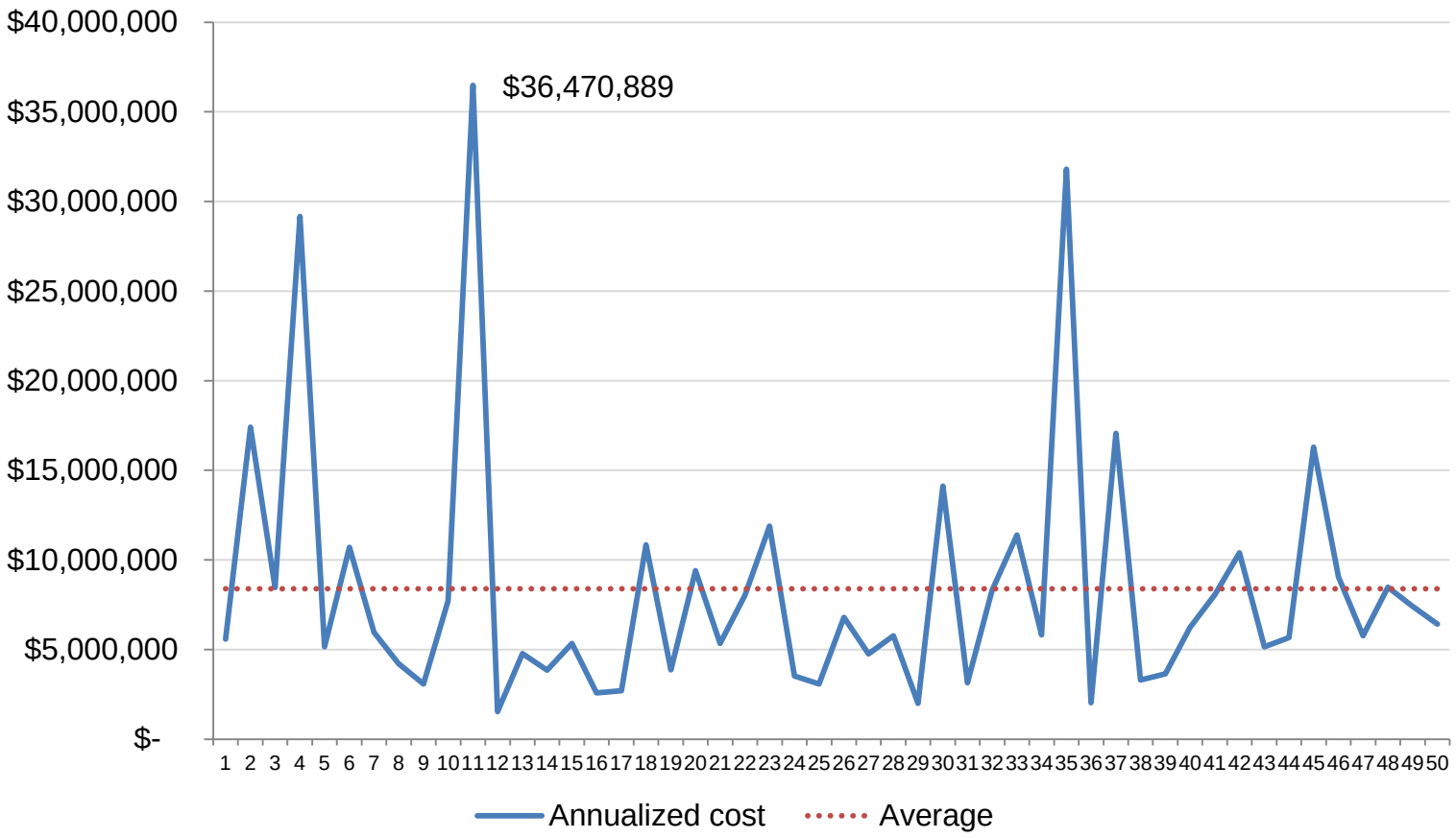


Organizational Cost Analysis

Annualized cost statistics

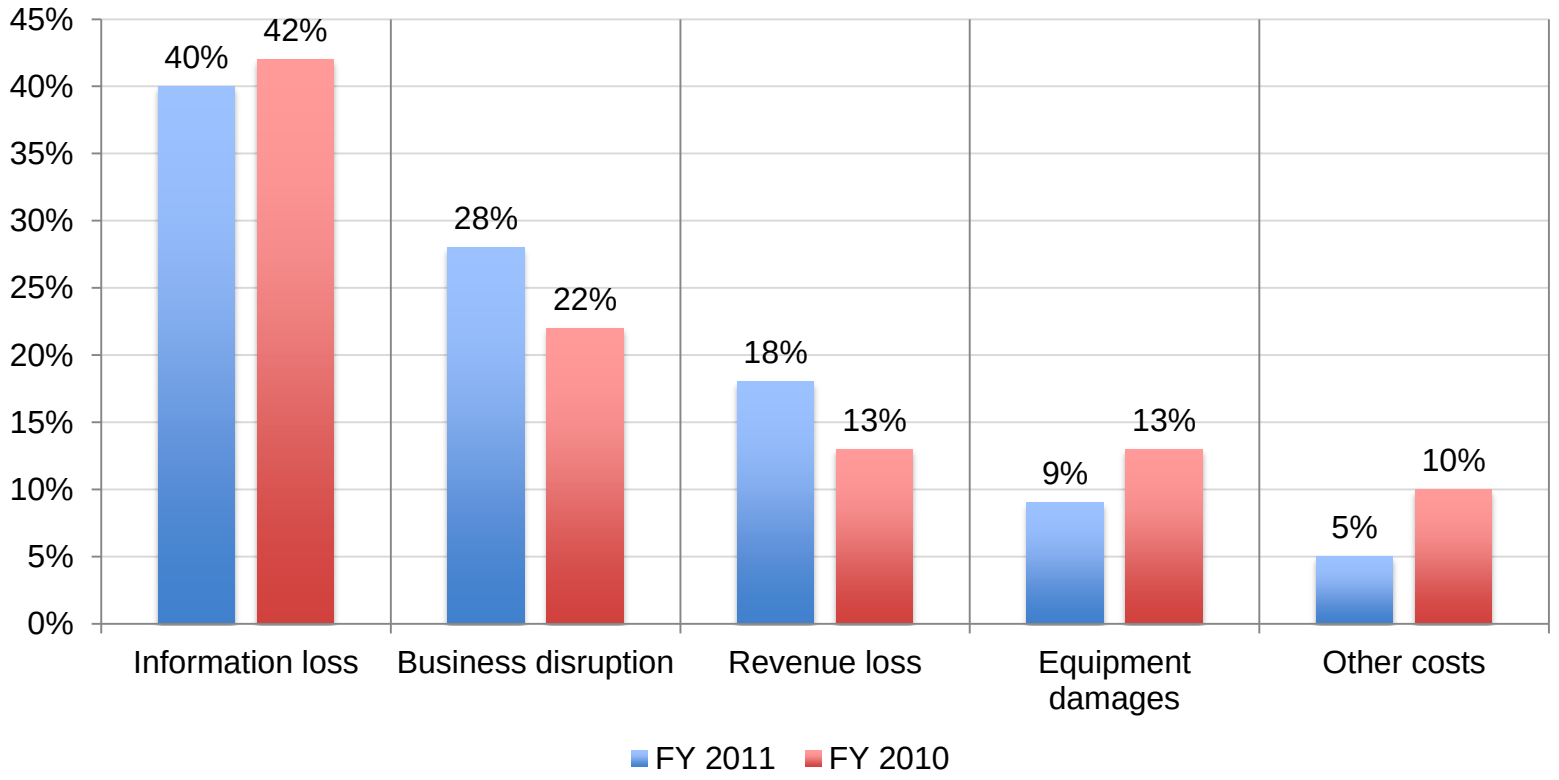


Annualized cost for 50 organizations



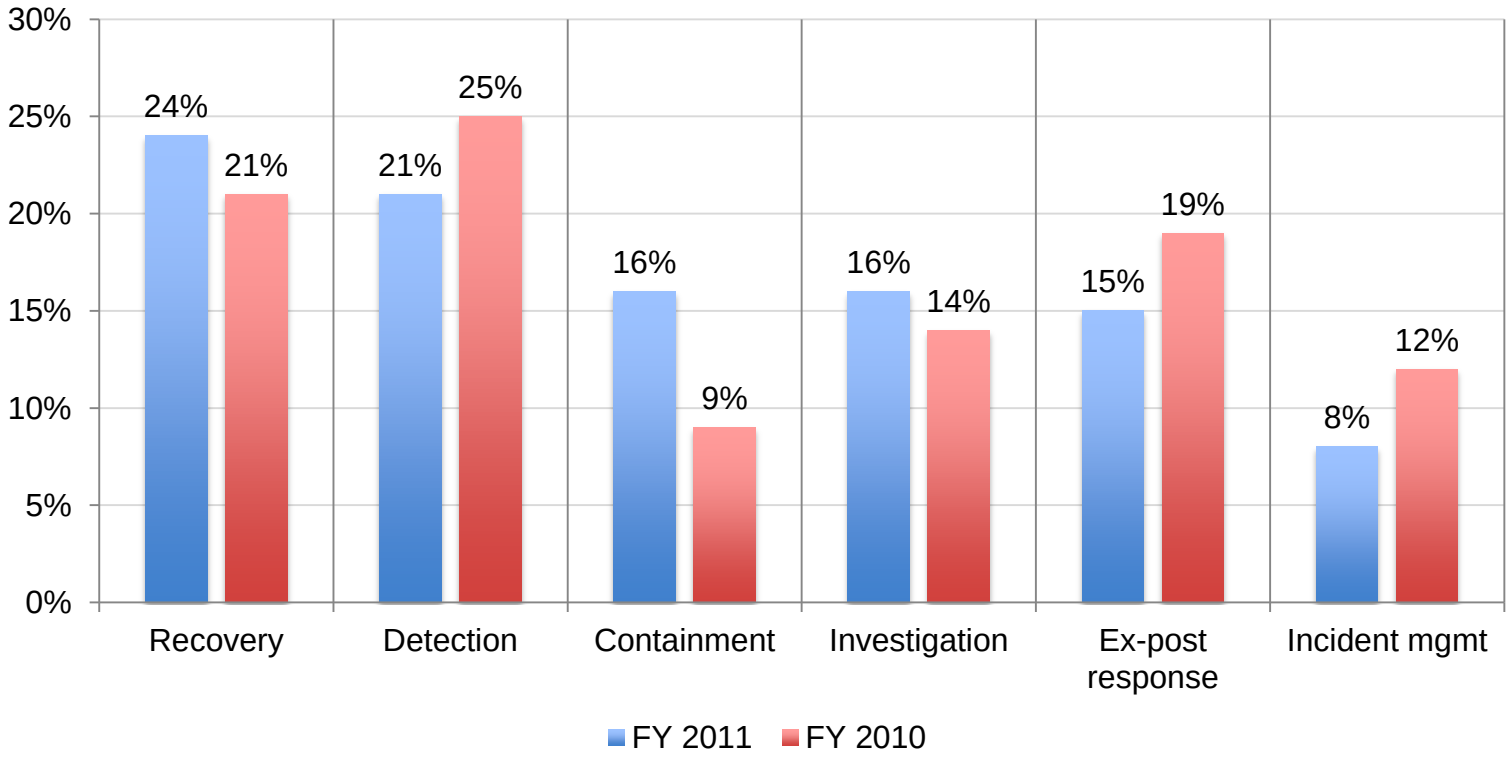
Percentage external costs

Other cost includes direct and indirect costs that could not be allocated to a main external cost category.

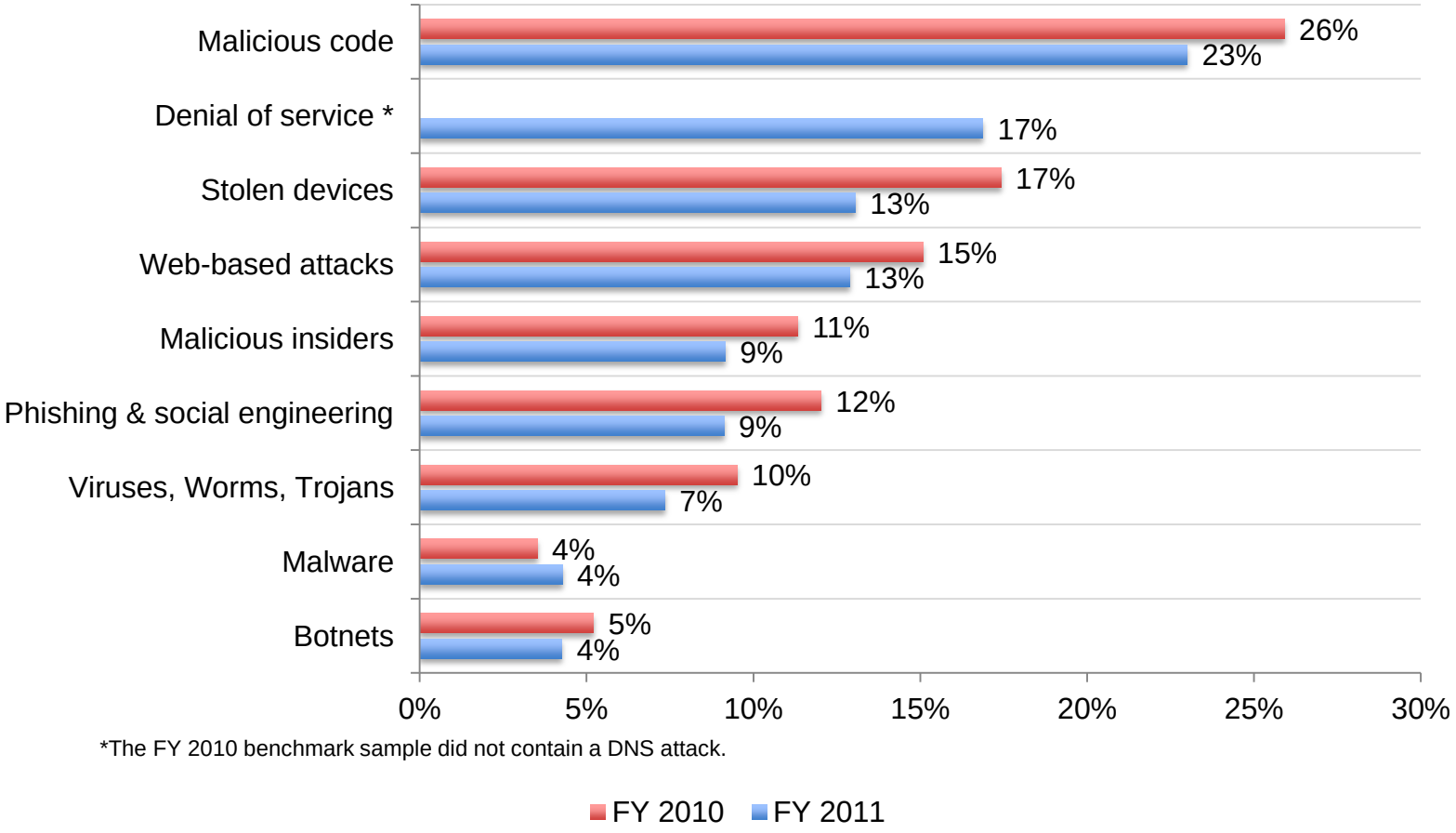


Percentage internal costs for six activity centers

Investigation and incident management are shown separately because their underlying cost drivers are different.

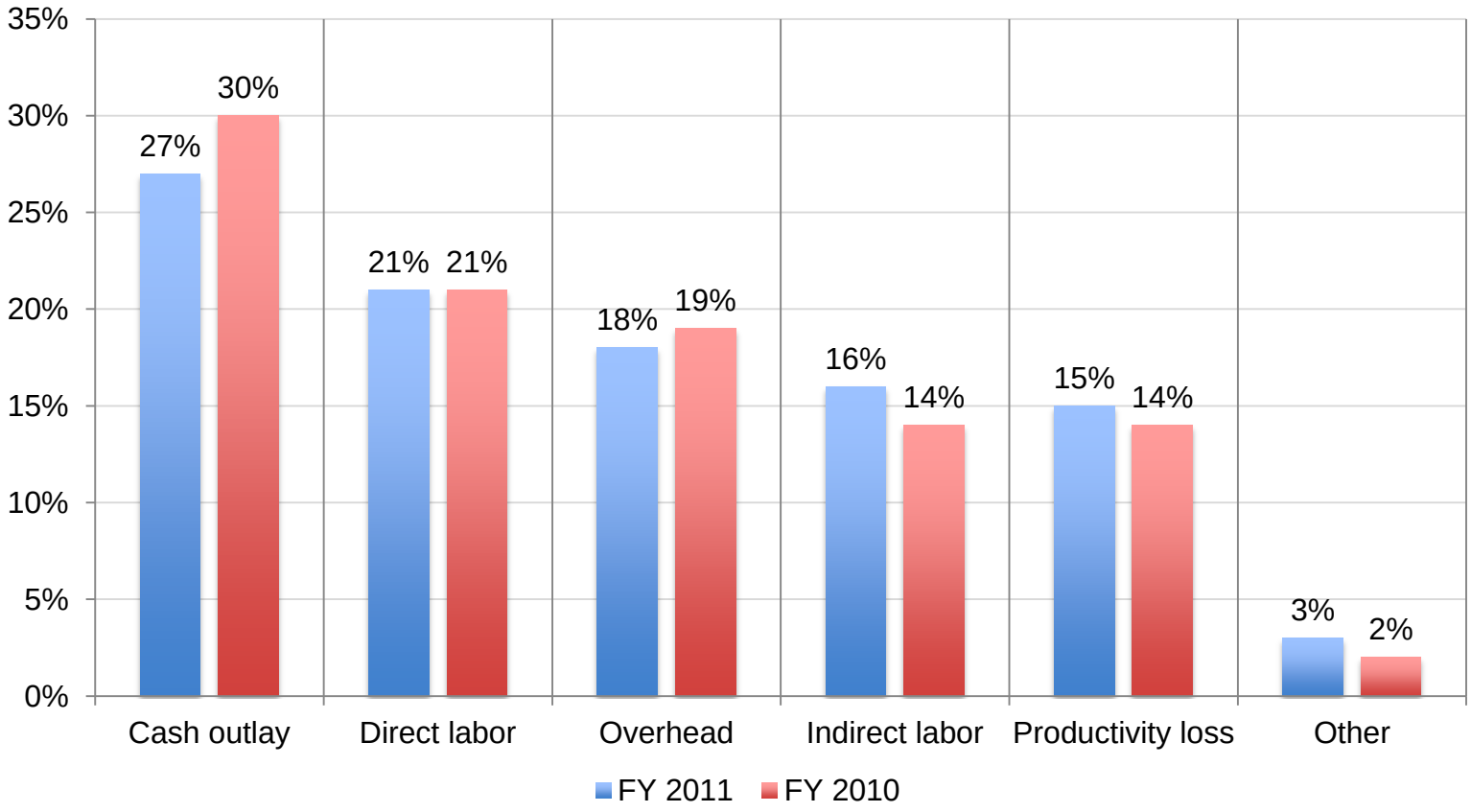


Percentage internal cost by attack type

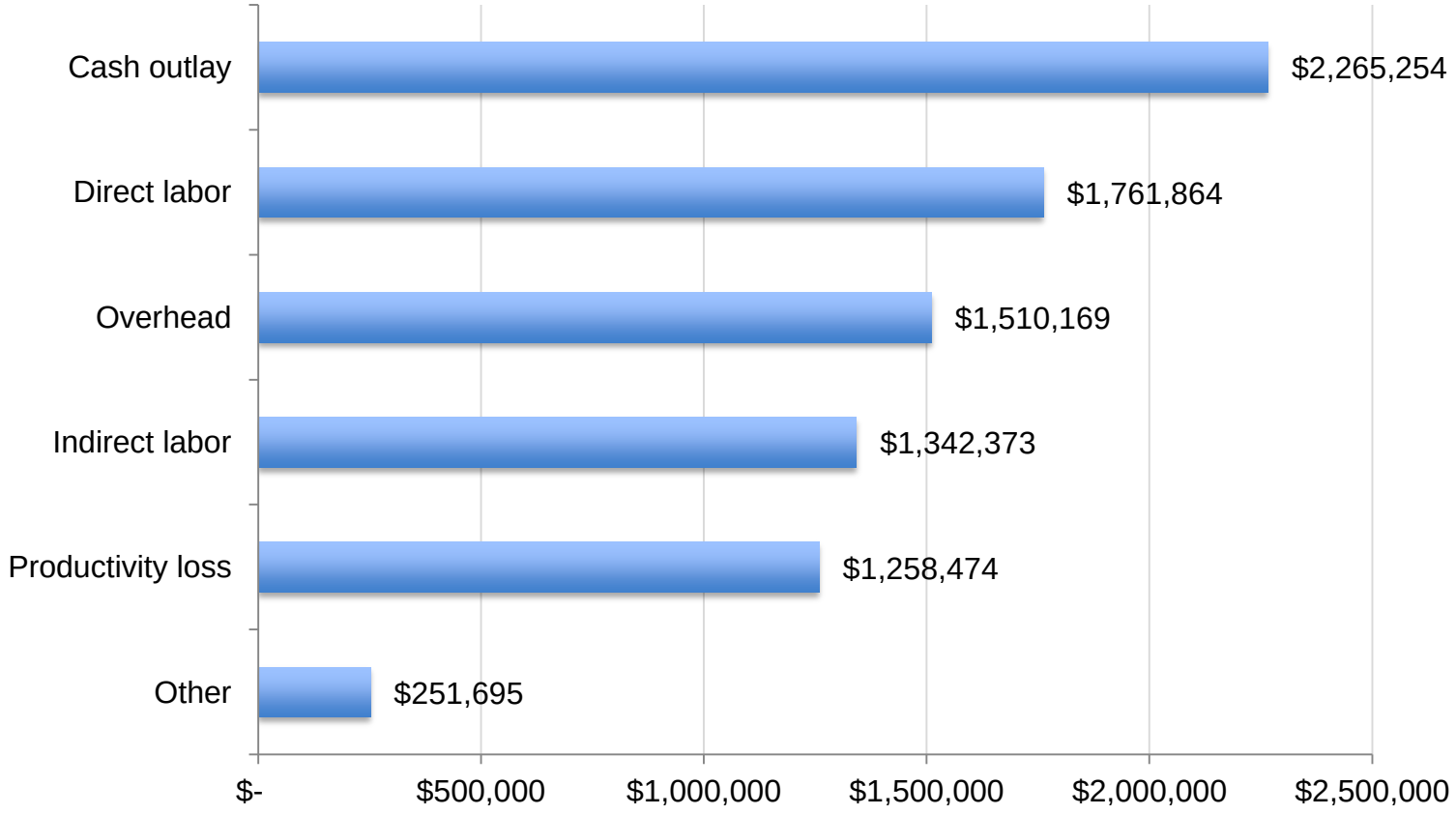


*The FY 2010 benchmark sample did not contain a DNS attack.

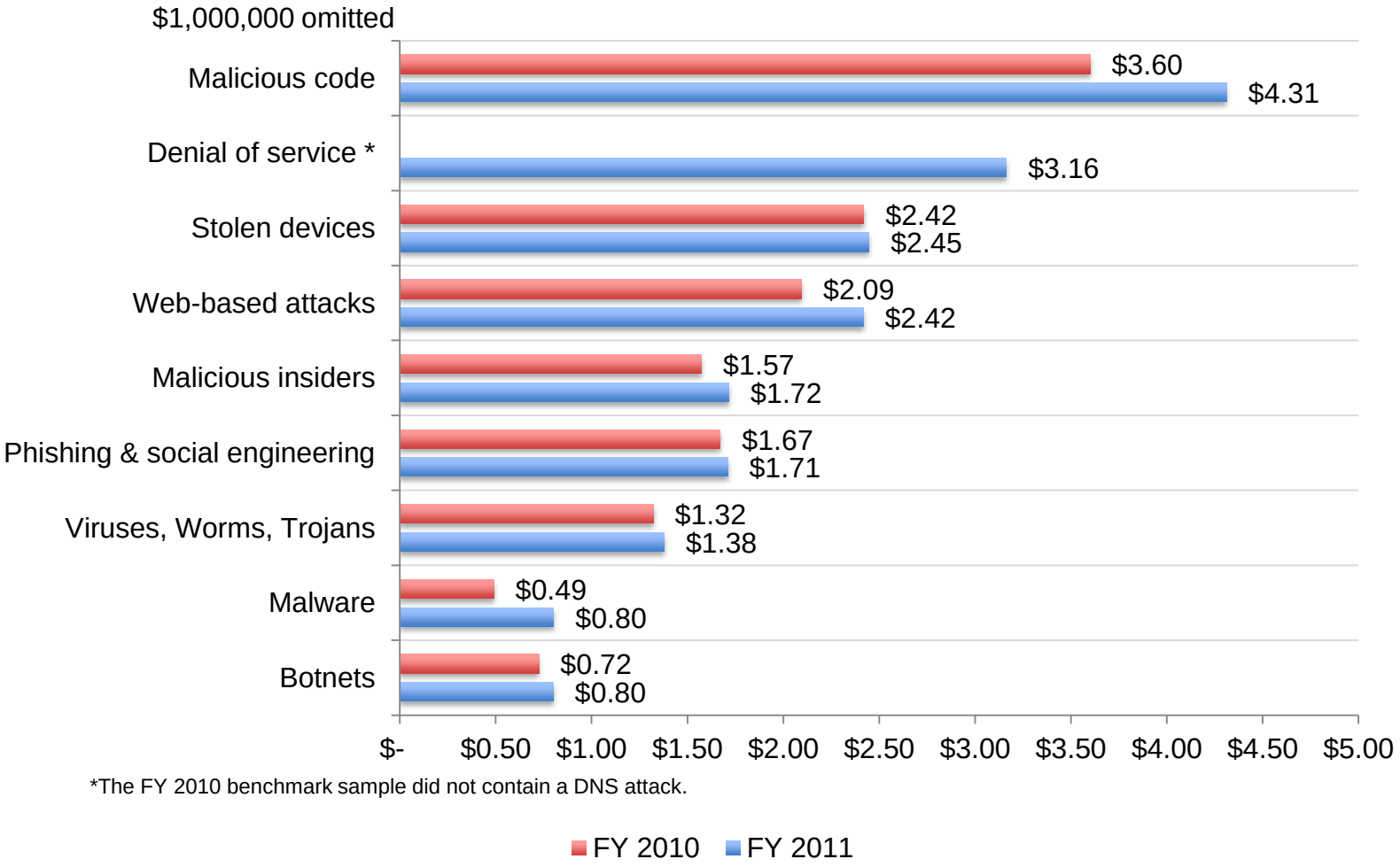
Percentage internal cost for six expense categories



Average internal cost for six expense categories

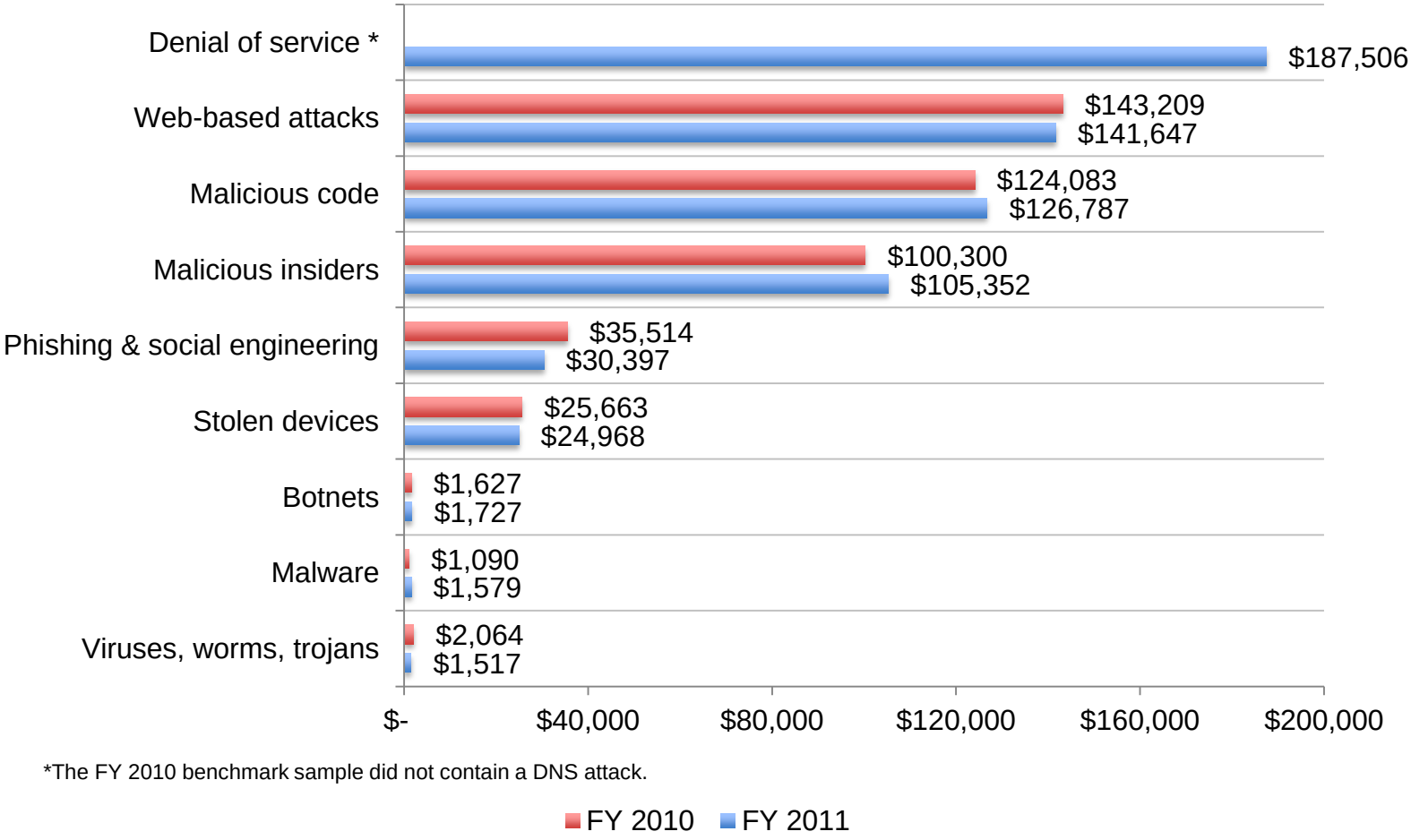


Annualized internal costs by attack type



*The FY 2010 benchmark sample did not contain a DNS attack.

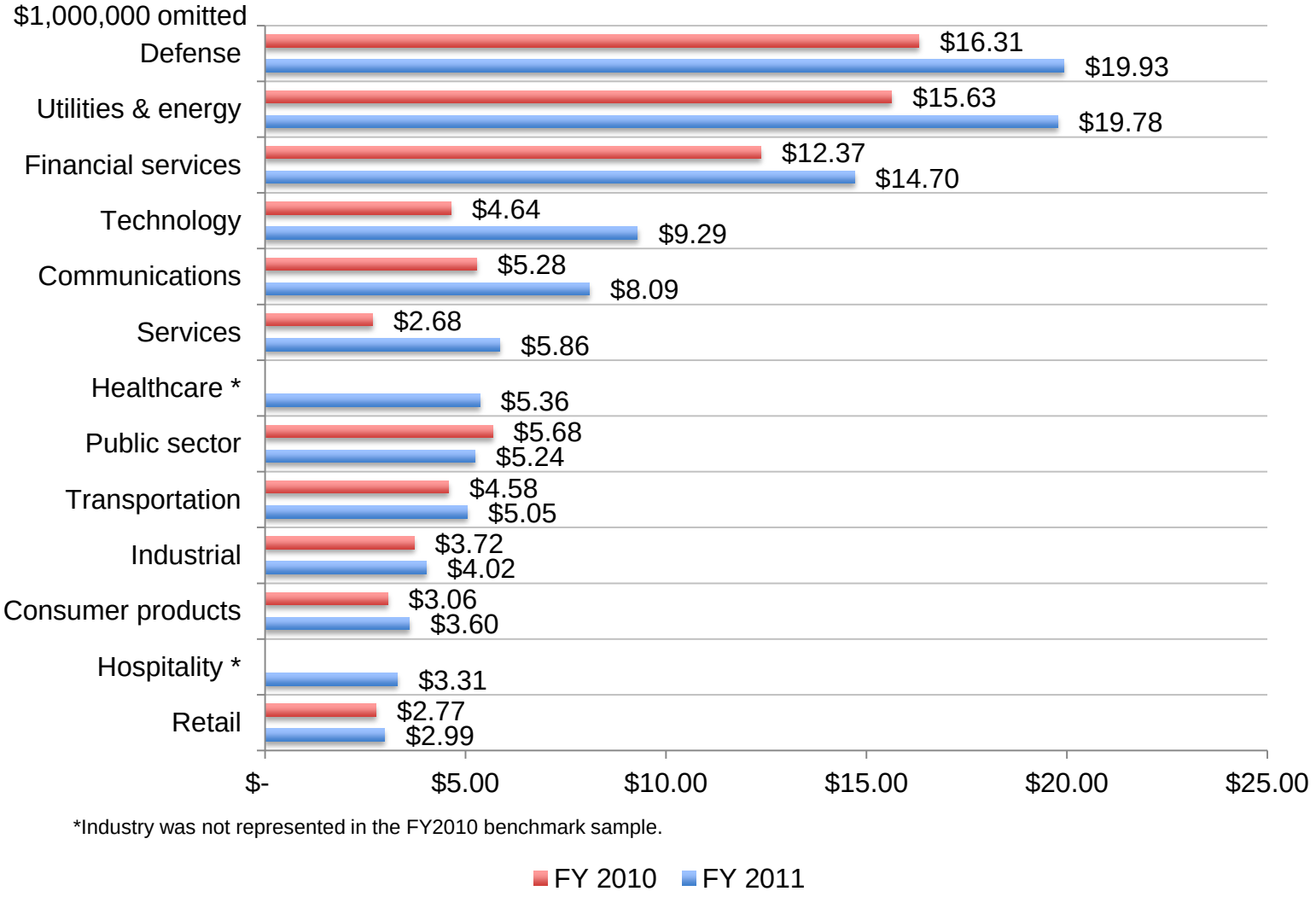
Annualized internal cost weighted by attack frequency



*The FY 2010 benchmark sample did not contain a DNS attack.

Annualized cost by industry sector

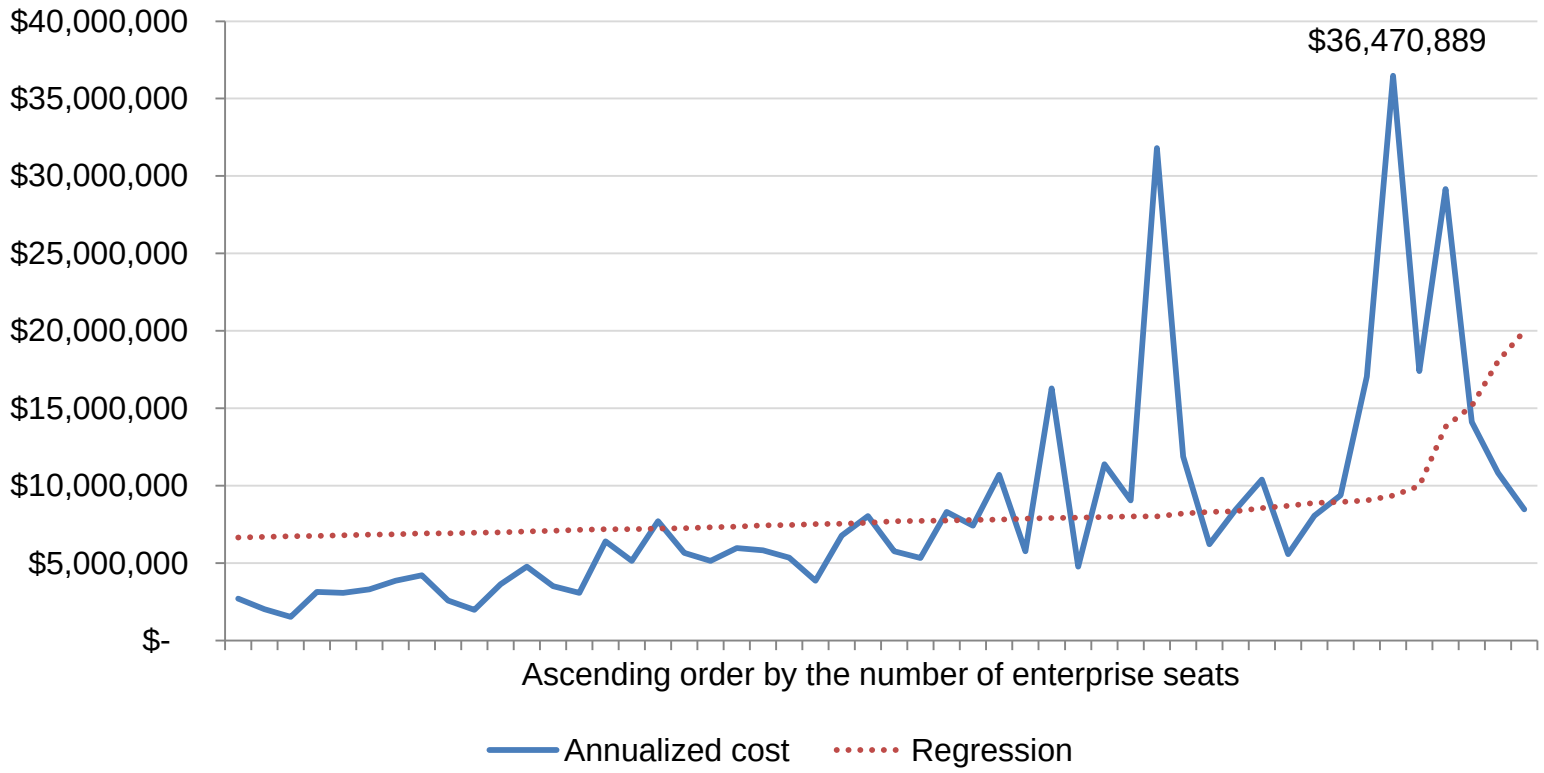
Due care should be exercised when reviewing industry differences because of small sample segment size.



*Industry was not represented in the FY2010 benchmark sample.

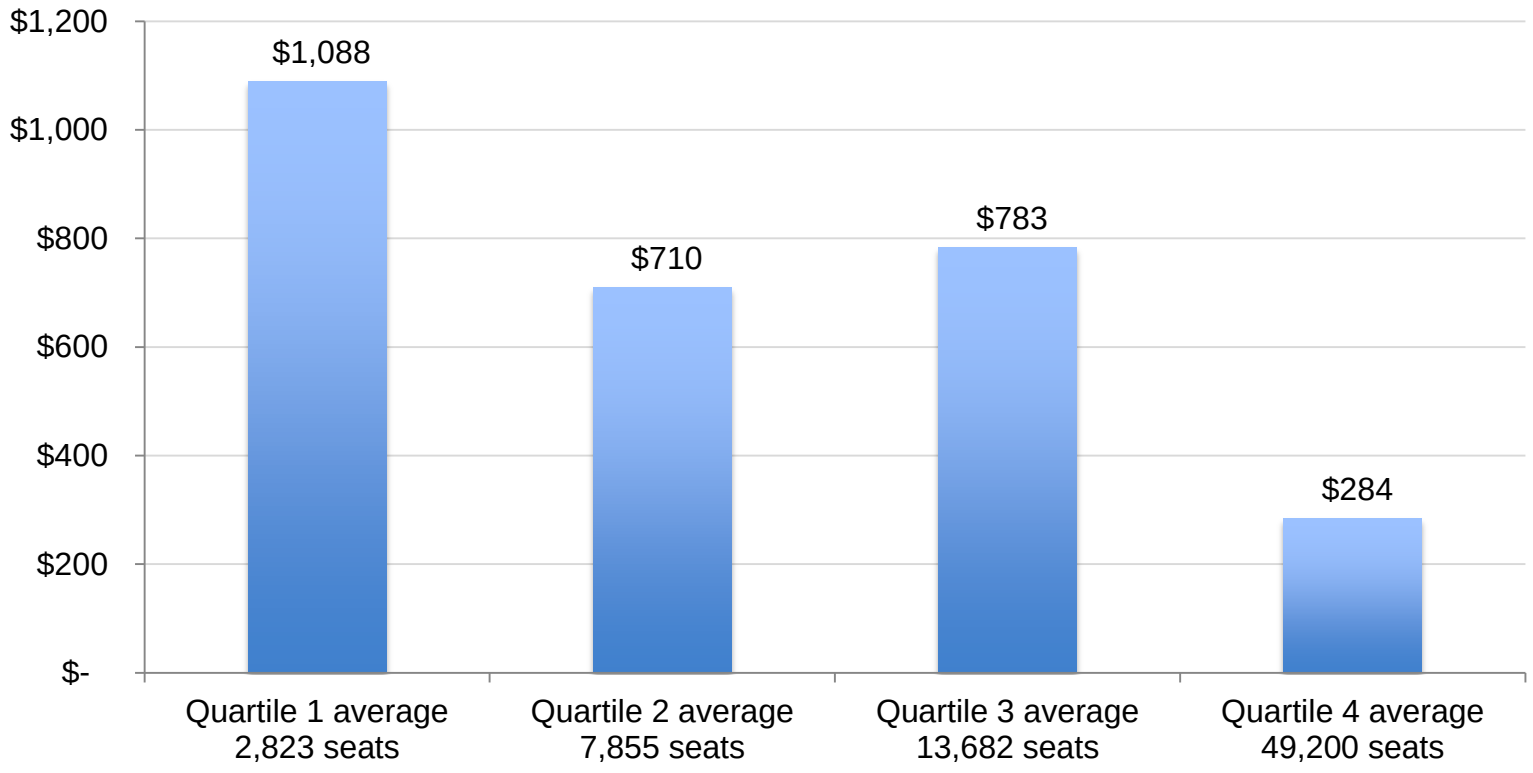
Annualized cost in ascending order by the number of enterprise seats

Regression performed on enterprise seats ranging from 700 to 139,200.



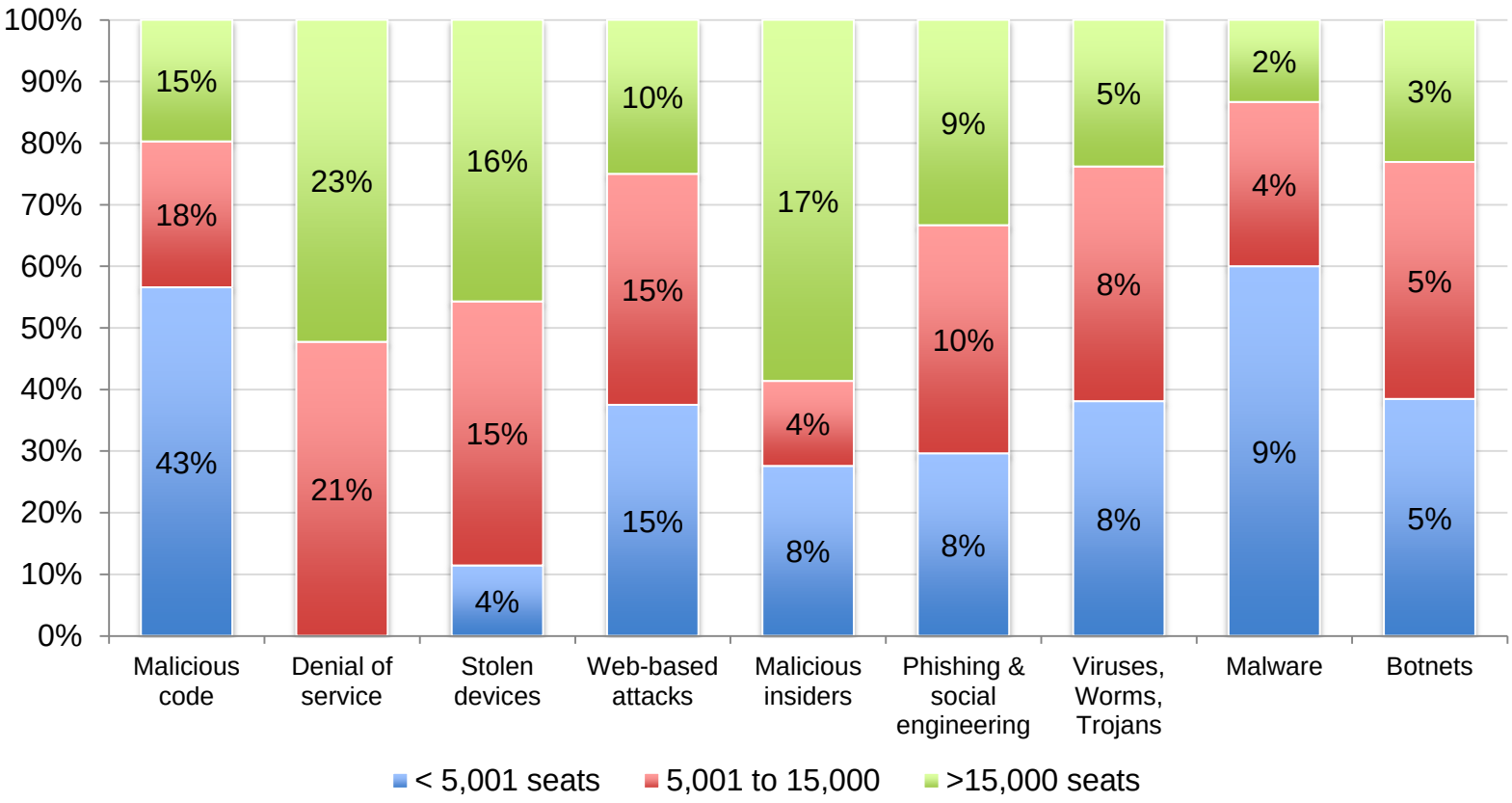
Quartile comparison of per capita cost by enterprise seats

Quartile 1 consists of the smallest sized organizations and Quartile 4 the largest sized organizations in terms of enterprise seats.



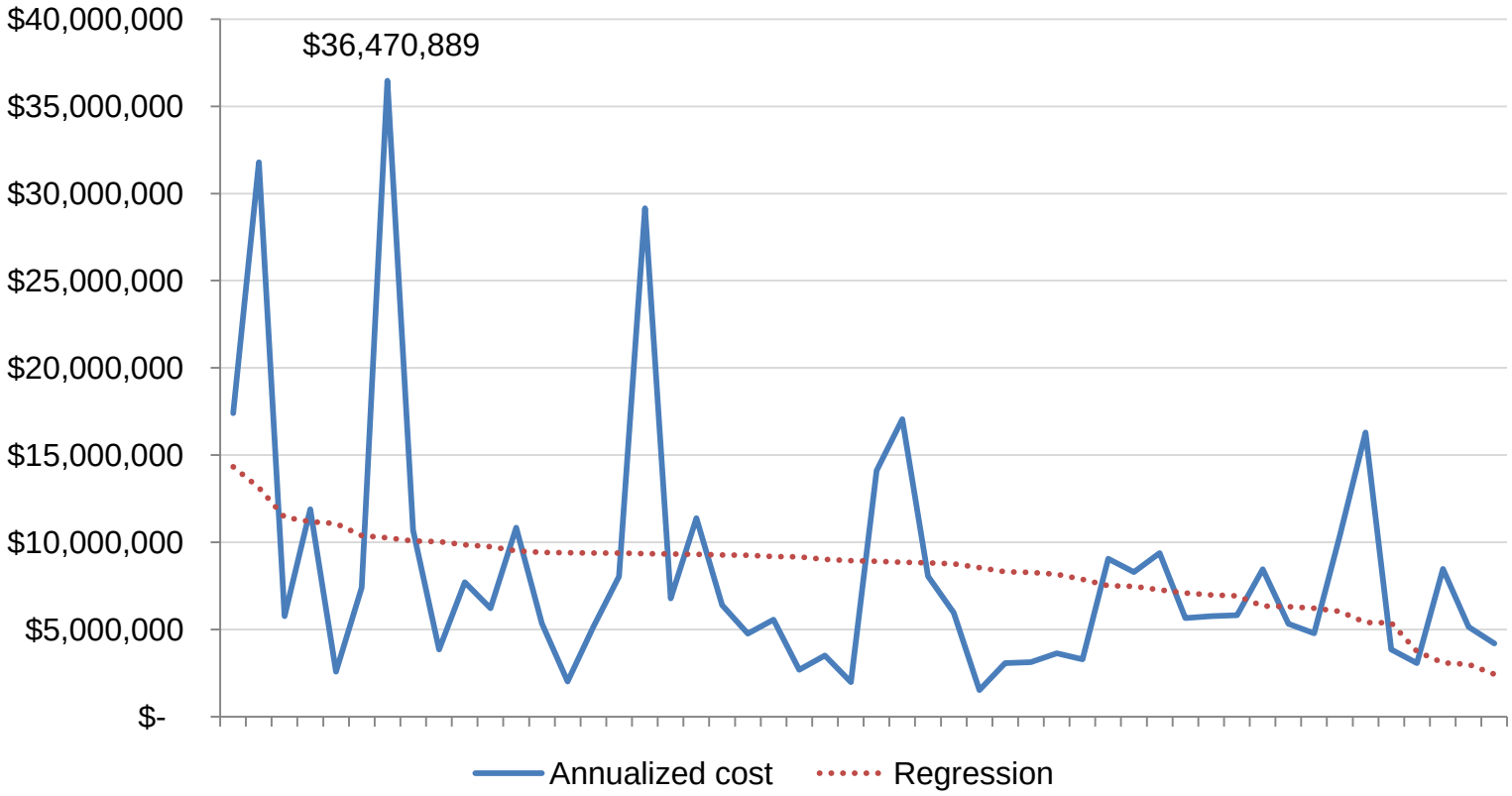
Cost mix by attacks and enterprise seats

Organizations are placed into three enterprise seat (size) ranges.



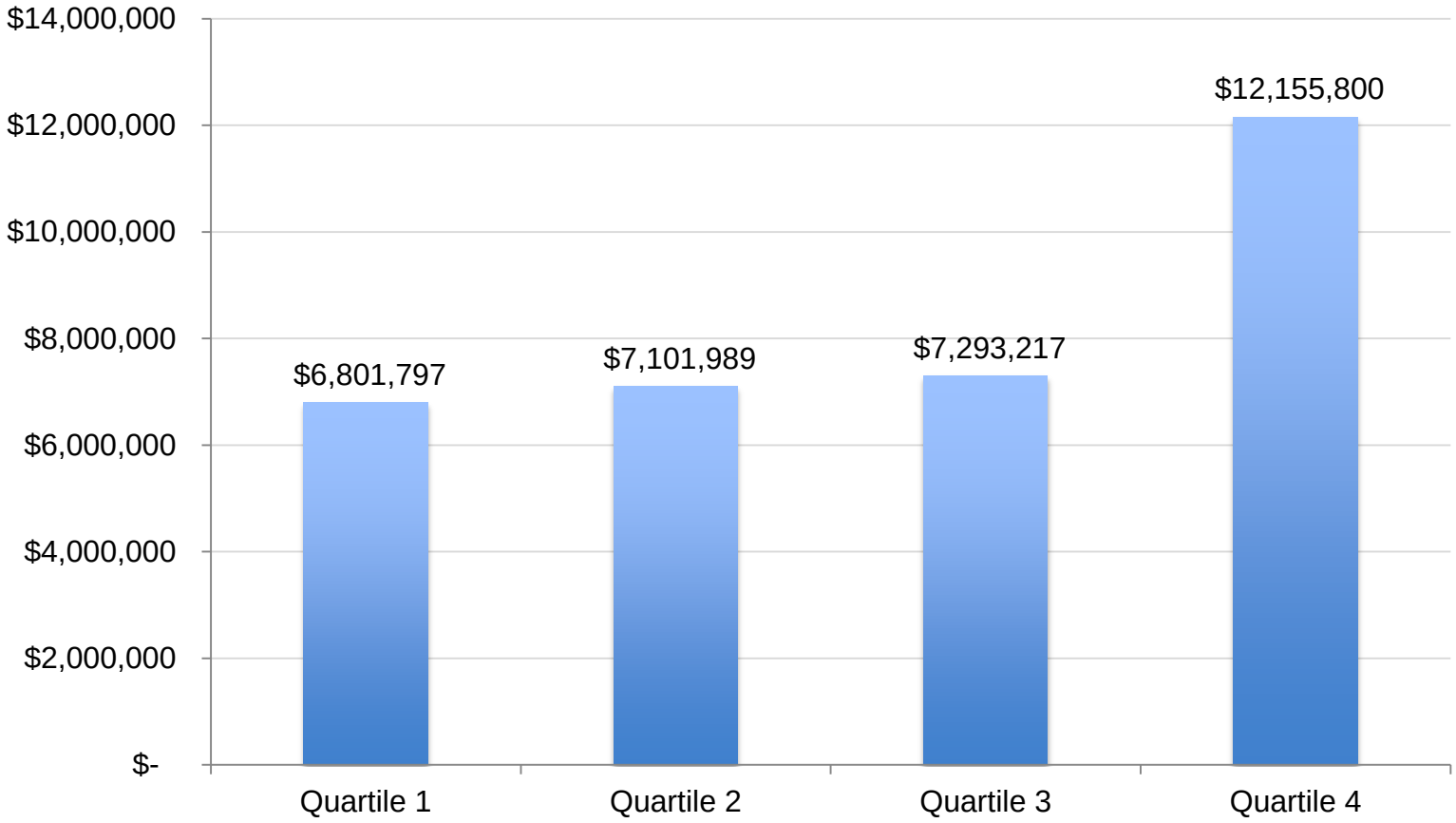
Inverse relationship between SES and annualized cost

Series ordered from lowest SES (-1.25) to highest SES (+1.77). Correlation (ρ) = -.32



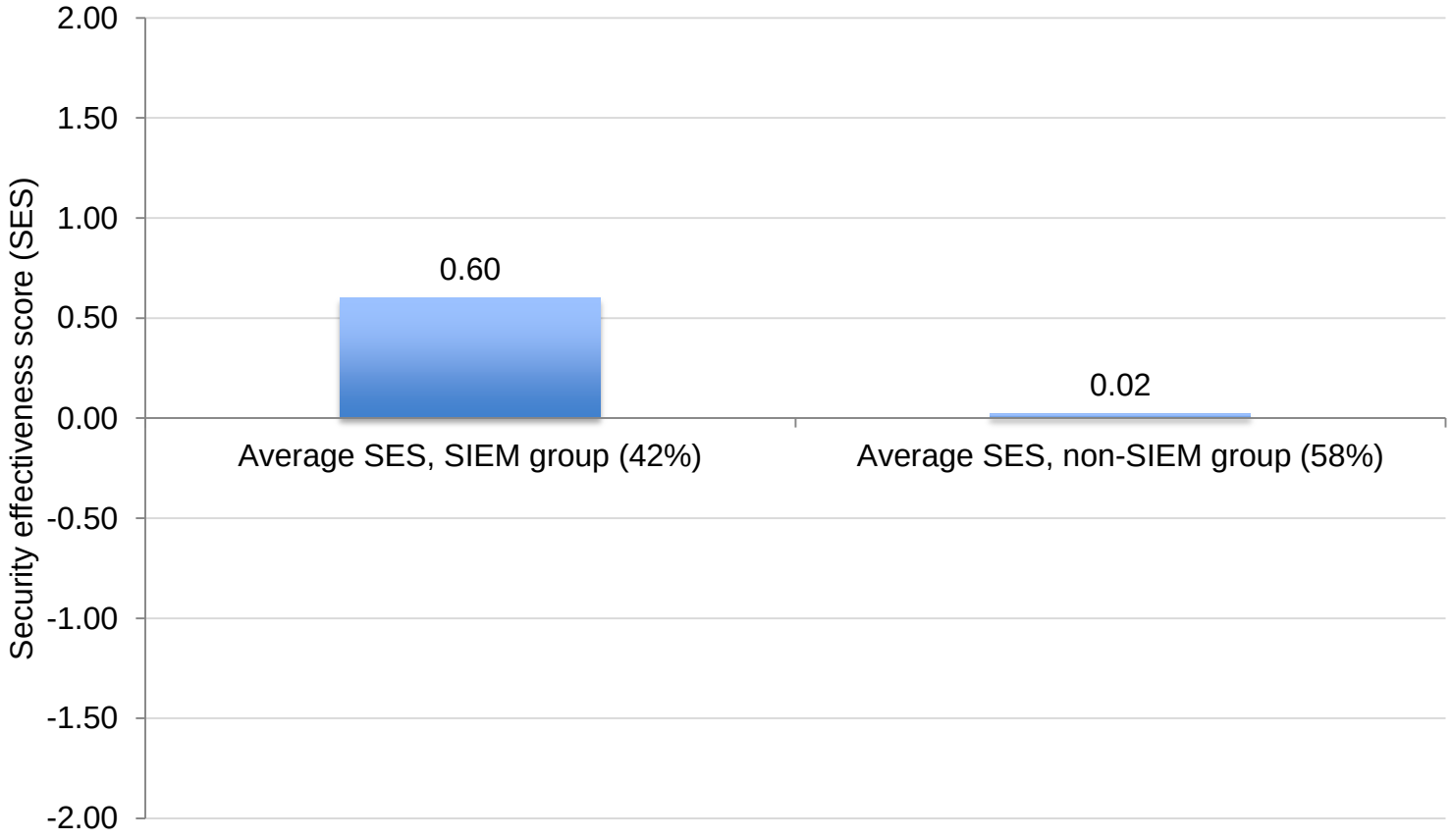
Quartile comparison of annualized cost by SES group

Average SES for Quartile 1 = +1.08, Quartile 2 = +.32, Quartile 3 = +.04 and Quartile 4 = -.35.



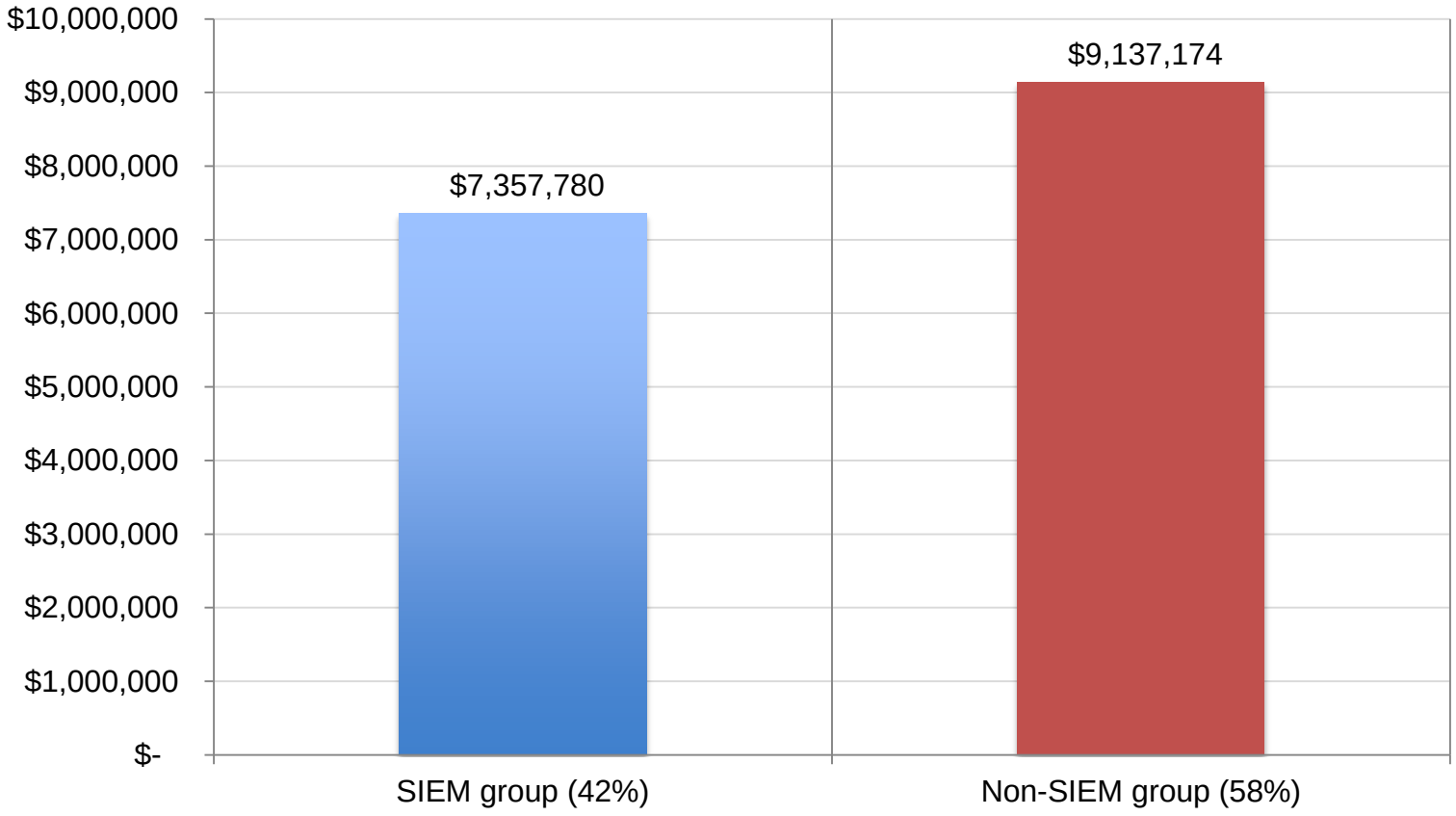
Comparison of SIEM and non-SIEM groups on average SES

The SES range for the benchmark sample is -1.25 (lowest) to +1.77 (highest).



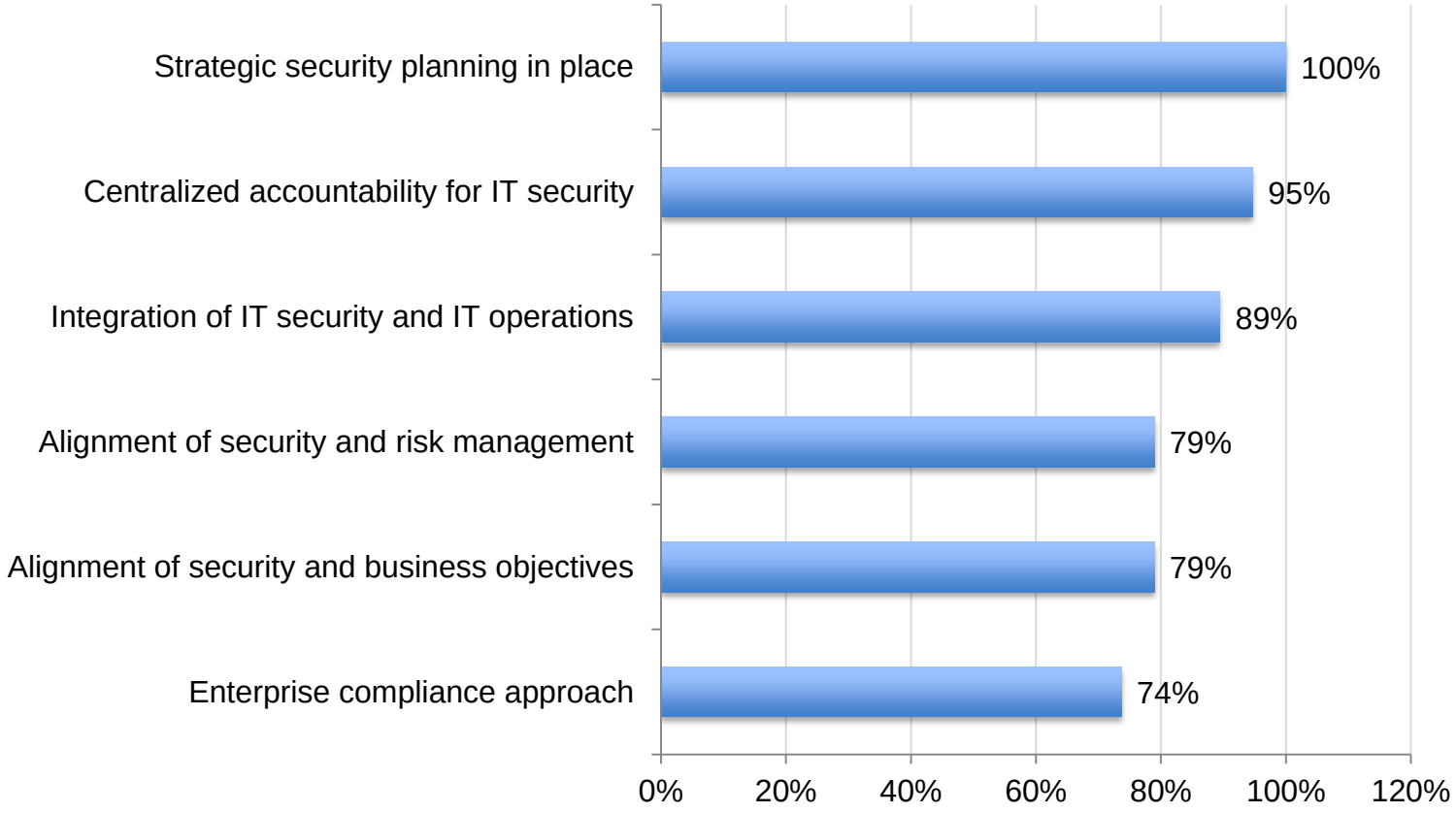
Comparison of SIEM and non-SIEM groups on average annualized cost

We determined that 21 (42%) of organizations deploy a SIEM or comparable network intelligence tools.



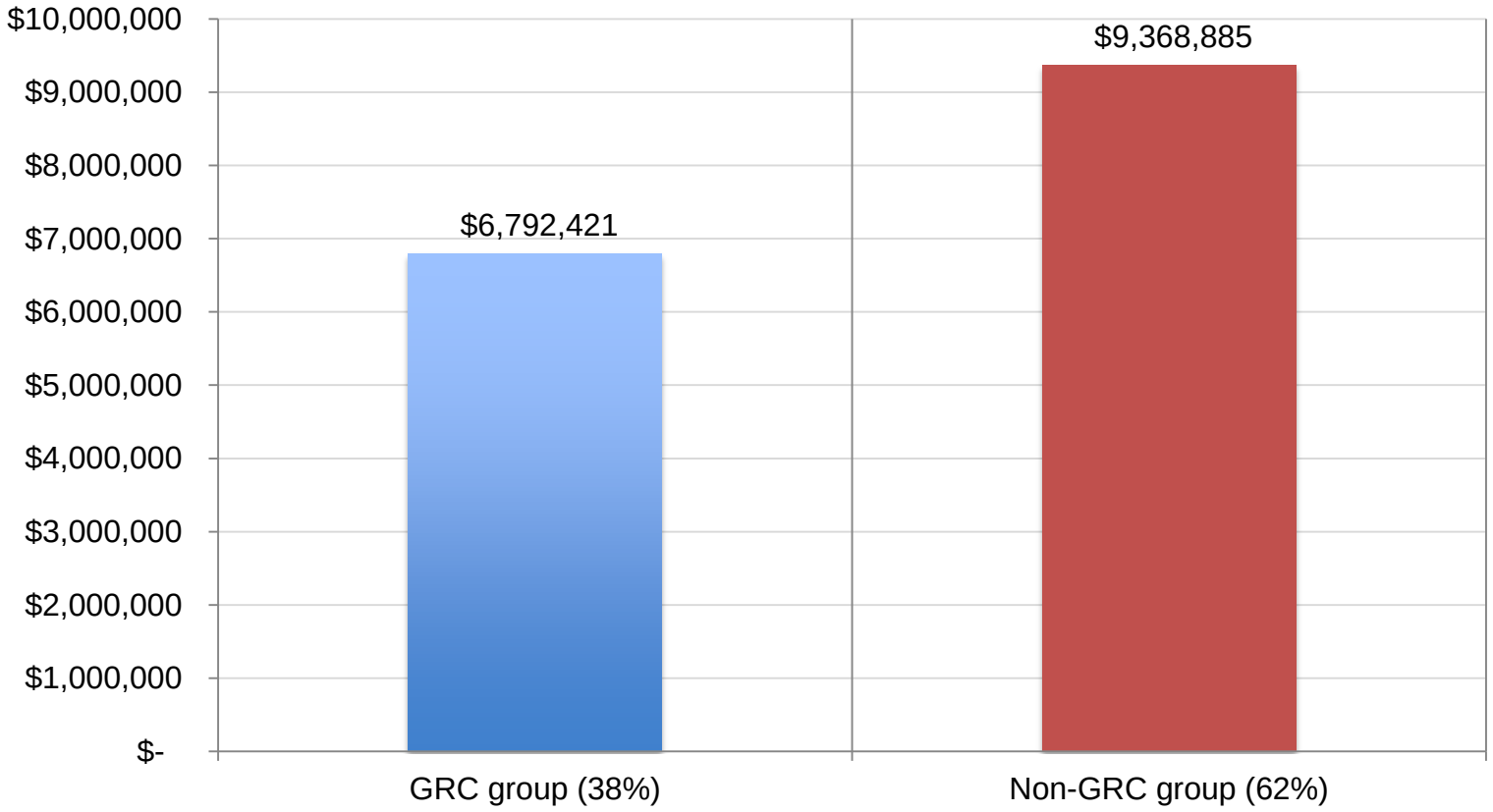
Characteristics of the GRC group

Based on diagnostic interview results, we determined that 19 (38%) of organizations deploy a GRC program. Following are their characteristics.



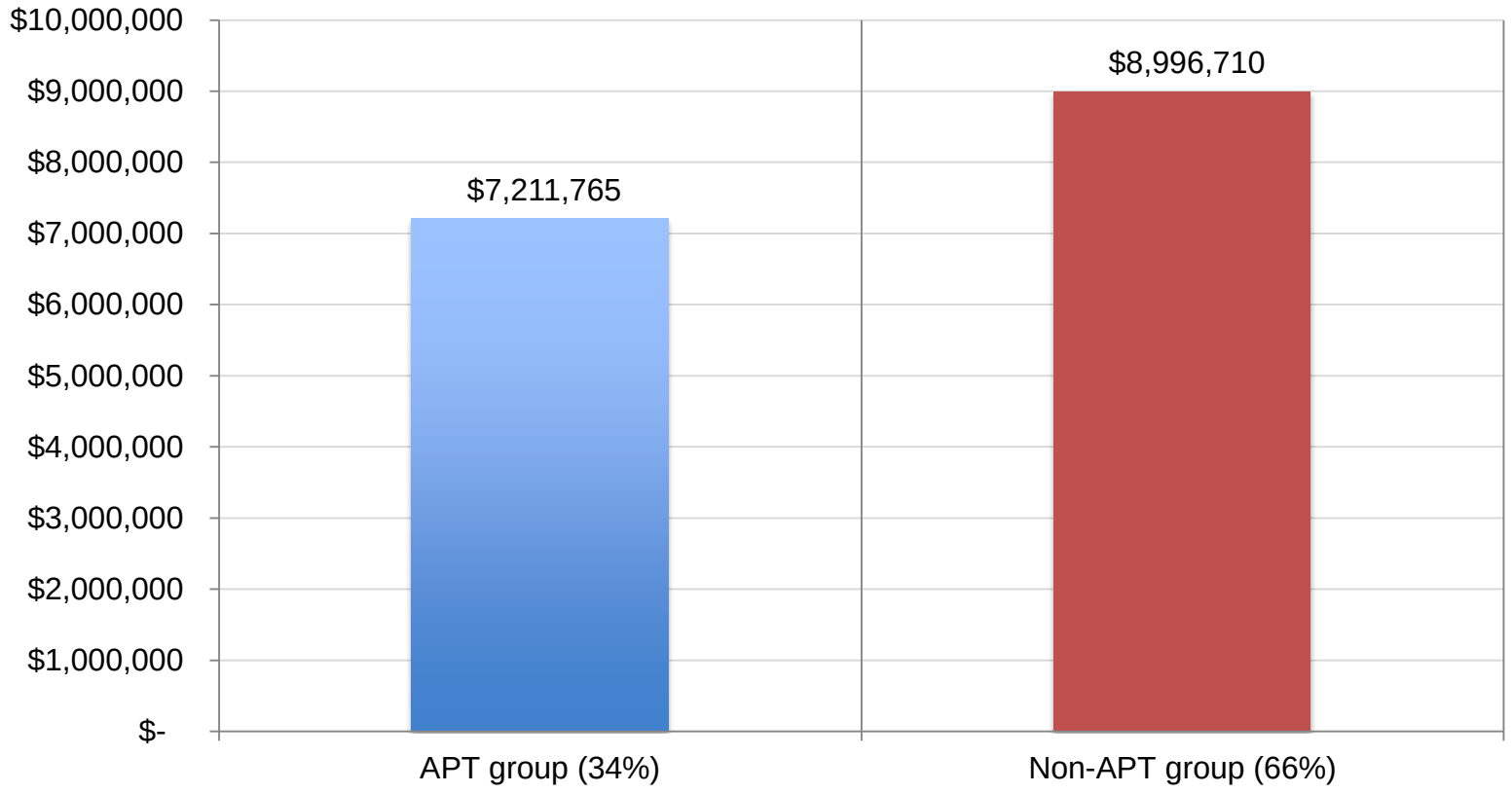
Comparison of GRC and non-GRC groups on average annualized cost

Based on diagnostic interview results, we determined that 19 (38%) of organizations deploy a GRC program. Following are their characteristics.



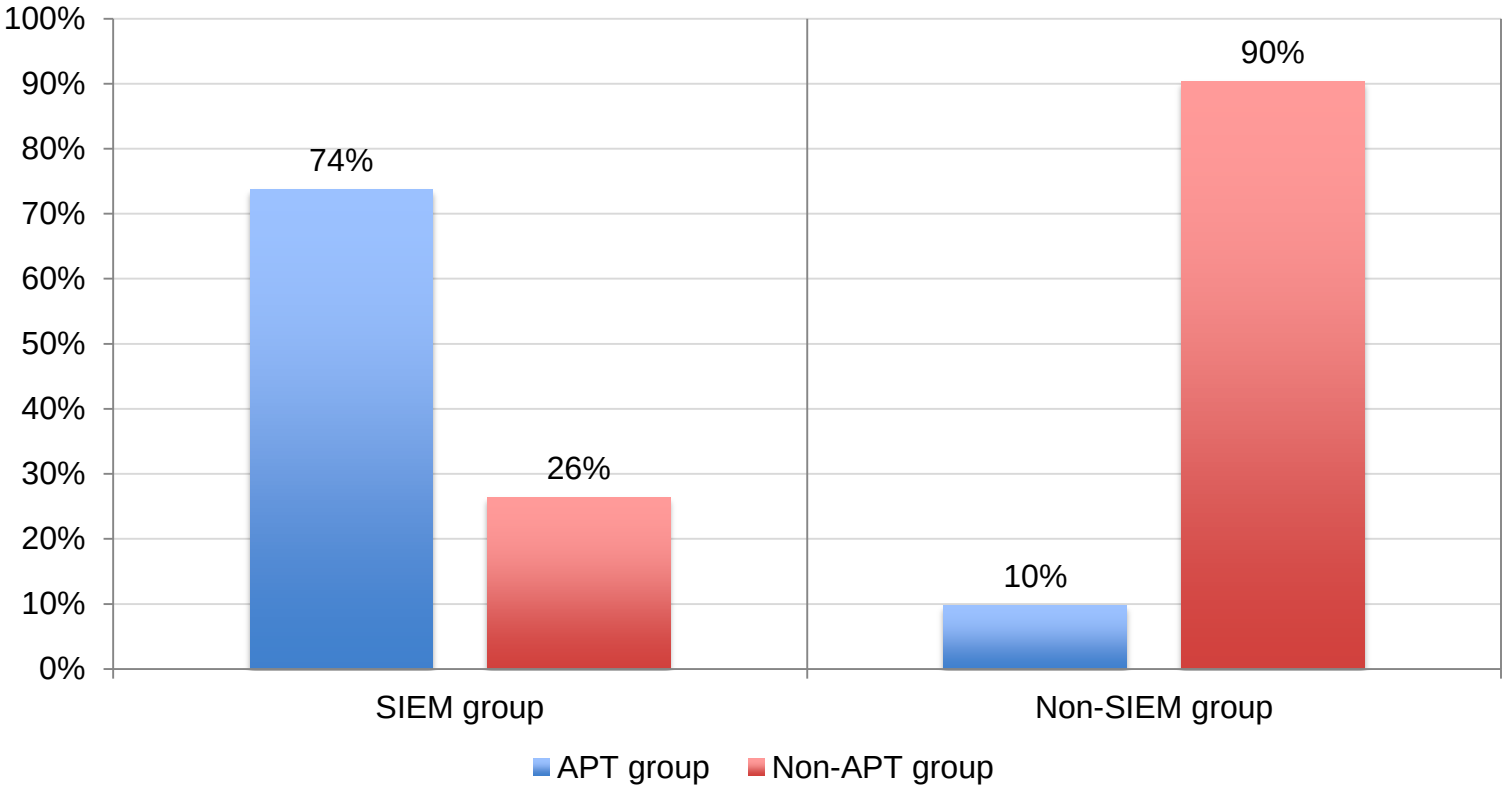
Comparison of APT and non-APT groups on average annualized cost

Based on diagnostic interview results, we determined that 17 (34%) of organizations recognized advance persistent threats (APT) during the field research period.



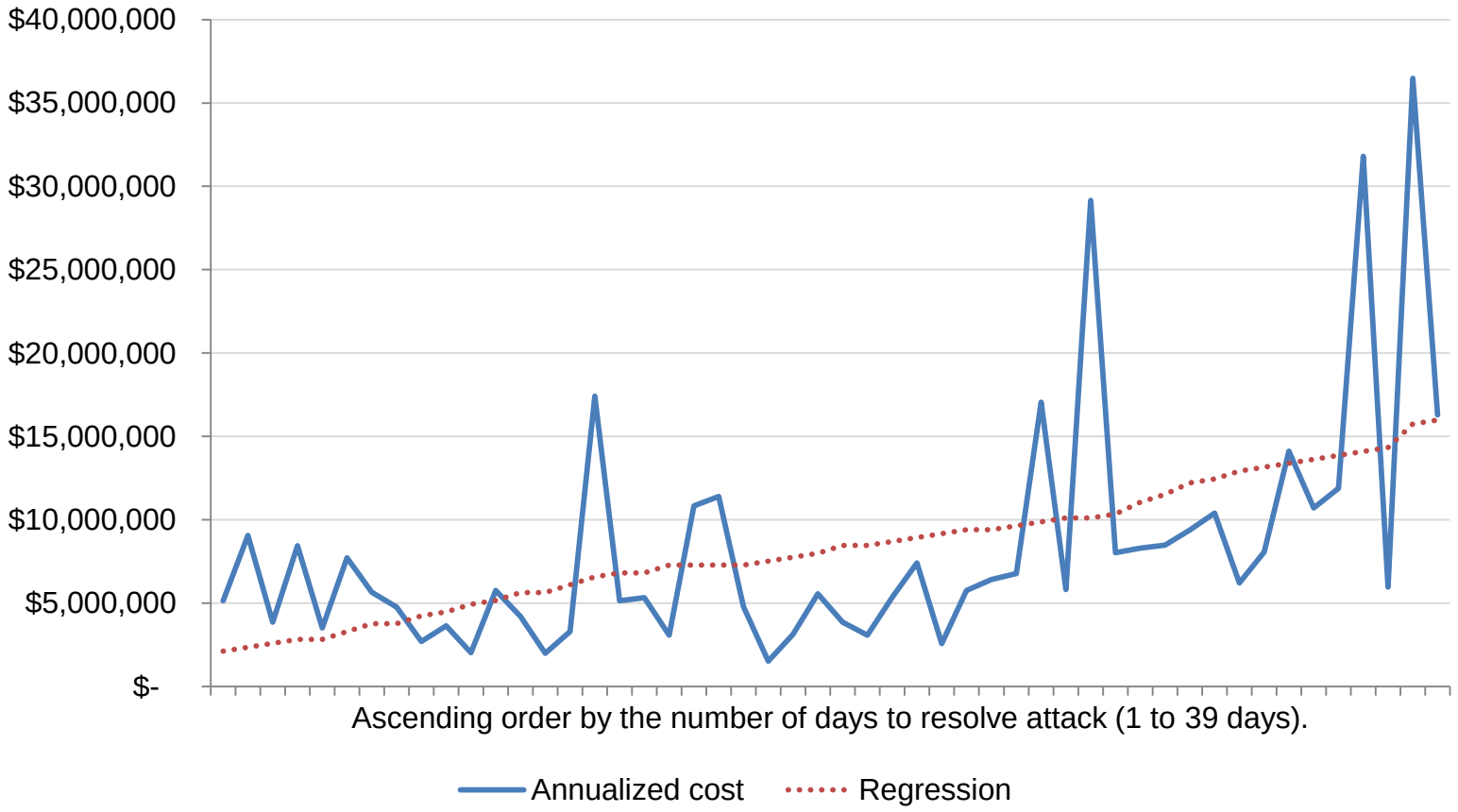
Interrelationship between SIEM and APT groups

As shown below, 74% of organizations in the SIEM group recognized APT activity during the field research period. In contrast, 90% of organizations in the non-SIEM group failed to recognize APT activity.



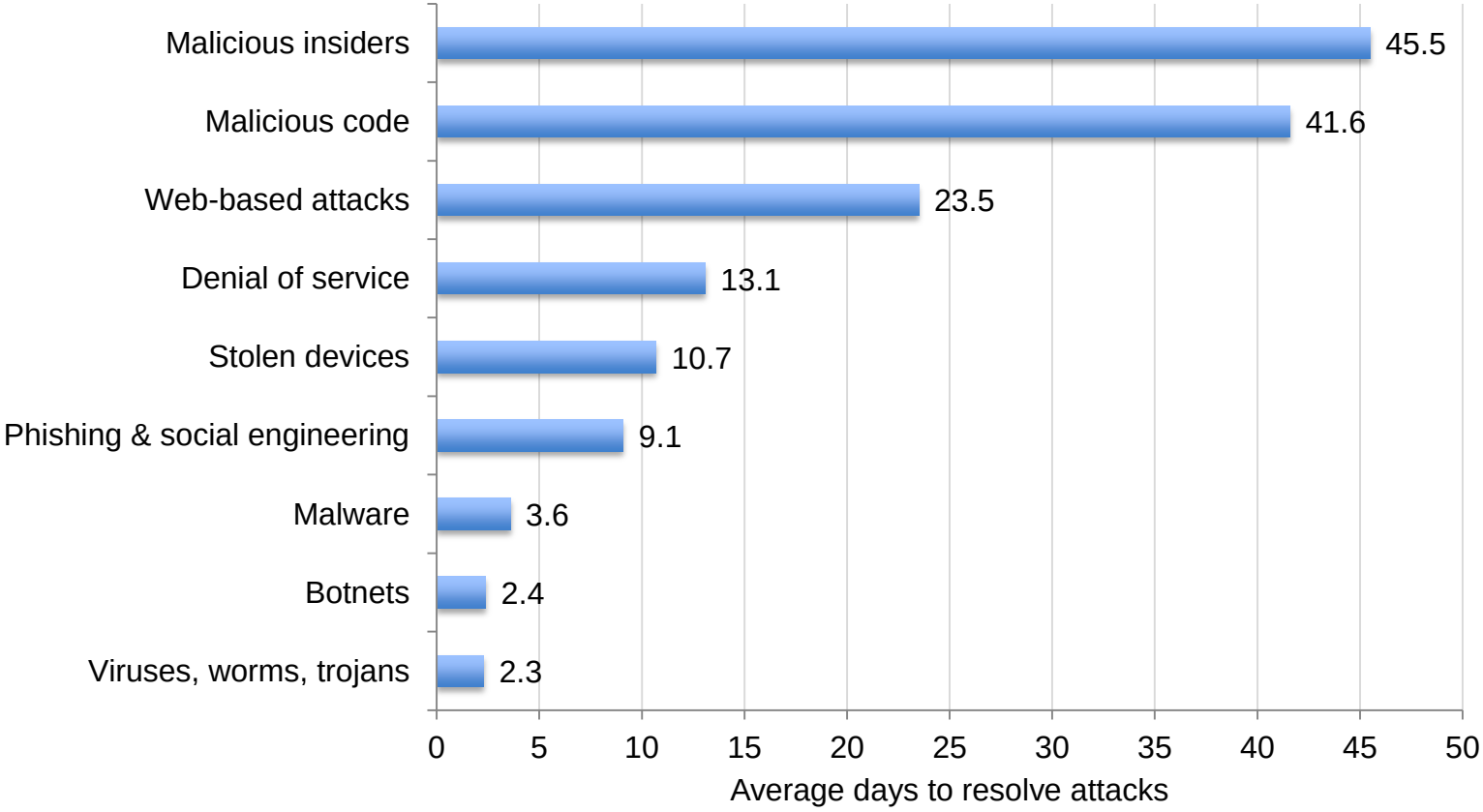
Annualized cost in ascending order by the number of days to resolve attacks

The estimated average days to resolve attacks is 18, with maximum at 39 days. The average cost to participating organizations of $415,748 over this 18-day period. This represents a 67 percent increase from last year's estimated average cost compiled for a 14 day period.

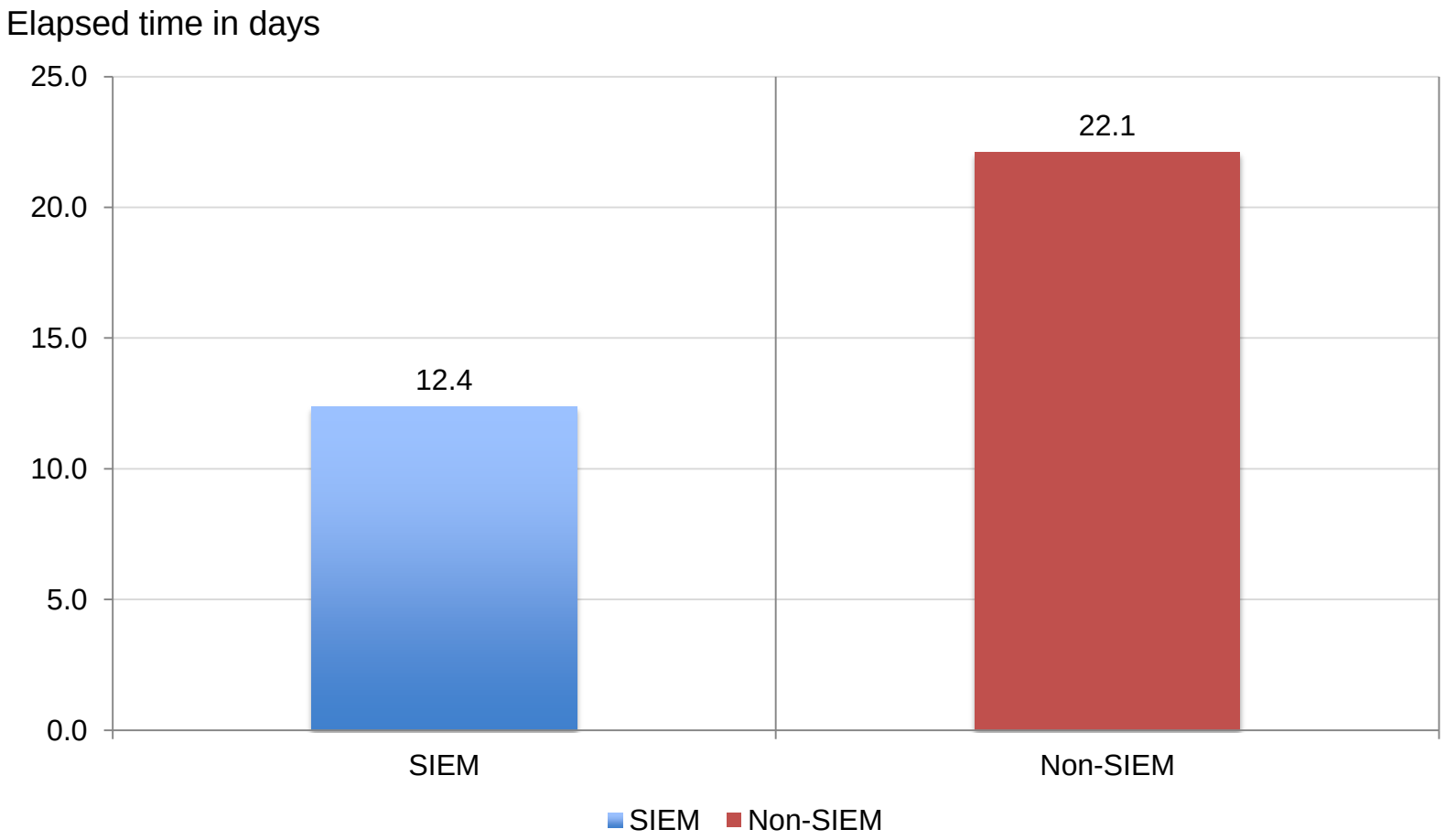


Average days to resolve attacks for nine attack types

Resolve is defined at the decision point where management declares the attack contained.



Average time to resolve attacks for SIEM and Non-SIEM groups



Caveats & Limitations

- There are inherent limitations to benchmark research that need to be carefully considered before drawing conclusions from findings.

- **Non-statistical results**: This study is descriptive. It draws upon a representative, non-statistical sample of organizations, all U.S.-based entities experiencing one or more cyber attacks during a four-week fielding period. Statistical inferences, margins of error and confidence intervals cannot be applied to these data given the nature of our sample.

- **Non-response**: The current findings are based on a small representative sample of completed organizational case studies. Fifty companies provided usable benchmark results. Non-response bias was not tested so it is always possible invited companies that did not participate are substantially different in terms of the methods used to manage the cyber crime containment and recovery process, as well as the underlying costs involved.

- **Sample bias**: Because our sampling frame is judgmental, the quality of results is influenced by the degree to which the frame is representative of the population of companies being studied. It is our belief that the current sampling frame is biased toward companies with more mature information security programs.

Caveats & Limitations - continued

- **Company-specific information**: The benchmark information is sensitive and confidential. Thus, the current instrument does not capture company-identifying information. It also allows individuals to use categorical response variables to disclose demographic information about the company and industry category. Industry classification relies on self-reported results.

- **Unmeasured factors**: To keep the survey concise and focused, we decided to omit other important variables from our analyses such as leading trends and organizational characteristics. The extent to which omitted variables might explain benchmark results cannot be estimated at this time.

- **Extrapolated cost results**. The quality of survey research is based on the integrity of confidential responses received from companies. While certain checks and balances can be incorporated into the survey process, there is always the possibility that respondents did not provide truthful responses. In addition, the use of a cost rather than actual cost data could create significant bias in presented results.

Questions?

Ponemon Institute
www.ponemon.org
Tel: 231.938.9900
Toll Free: 800.887.3118
Michigan HQ: 2308 US 31 N. Traverse City, MI 49686
research@ponemon.org